INVOLUTIONS ON ZILBER FIELDS

VINCENZO MANTOVA

Abstract. After recalling the definition of Zilber field, and the main conjecture behind them, we prove that Zilber fields of cardinality up to the continuum have involutions, i.e., automorphisms of order two analogous to complex conjugation on $\mathbb{C}_{\exp}$. Moreover, we also prove that for continuum cardinality there is an involution whose fixed field, as a real closed field, is isomorphic to the field of real numbers, and such that the kernel is exactly $2\pi i\mathbb{Z}$, answering a question of Zilber, Kirby, Macintyre and Onshuus.

The proof is obtained with an explicit construction of a Zilber field with the required properties. As further applications of this technique, we also classify the exponential subfields of Zilber fields, and we produce some exponential fields with involutions such that the exponential function is order-preserving, or even continuous, and all of the axioms of Zilber fields are satisfied except for the strong exponential-algebraic closure, which is replaced by some weaker axioms.

Contents

1. Introduction

Zilber fields are a recent creation of Boris Zilber [8] born during the study of the model theory of exponential maps, and mainly of $\mathbb{C}_{\exp}$. Indeed, a Zilber field is first of all a structure $(K, 0, 1, +, \cdot, E)$, where K is a field and E is an exponential function, i.e., a map satisfying

$$E(x + y) = E(x) \cdot E(y).$$

Date: Draft of September 29, 2011.

A certain number of axioms must hold for the structure to be a Zilber field. In analogy with the classical cases of $\mathbb{C}_{\exp}$ and $\mathbb{R}_{\exp}$, we will denote by "K_E" the structure made up by a field K and an exponential function E in the above sense. The function E of a Zilber field is called *pseudoexponentiation*.

The axioms of Zilber fields state that K_E must be somewhat similar to the structure $\mathbb{C}_{\exp}$, but also forces it to have some properties that are deep conjectures for the classical exponential function. Schanuel's Conjecture, rephrased with E in place of exp, is included among these axioms.

The remarkable result by Zilber [8] is that these axioms are quite simply expressible in a suitable infinitary language and more importantly they are *uncountably categorical*. In Zilber's philosophy, categorical structures should correspond to natural mathematical objects, so he conjectured that $\mathbb{C}_{\exp}$ is exactly the model of cardinality $2^{\aleph_0}$. The unique model of cardinality $2^{\aleph_0}$ has been called "$\mathbb{B}$" by Macintyre, after Boris Zilber. Here we will use the variant "$\mathbb{B}_E$" when we want to explicitly name the pseudoexponential function.

It is quite natural to ask which properties of $\mathbb{C}_{\exp}$ we are able to prove on Zilber fields, and especially on $\mathbb{B}$. In particular, it has been asked recently in various forms by Kirby [3], Macintyre, Onshuus [4], Zilber and others if Zilber fields feature a 'pseudoconjugation', i.e., an automorphism of order two, or in other words an involution; and it has been also asked if we can make the pseudoexponentiation increasing on the fixed field of the involution, which is automatically an ordered real closed field. It is known that Zilber fields have many automorphisms, but not if there is an involution, and on the other hand, the only automorphism of $\mathbb{C}_{\exp}$ that we know of is complex conjugation.

Moreover, the involution of $\mathbb{C}_{\exp}$ plays a rather important role, as we can use it to give a simple definition of exp: it is the unique exponential function commuting with complex conjugation and continuous with respect to the induced topology such that $\exp(1) = e$, $\ker(\exp) = 2\pi i\mathbb{Z}$ and $\exp(i\frac{\pi}{2}) = i$. A possible way then to prove that $\mathbb{C}_{\exp} \cong \mathbb{B}_E$ would be finding an involution of $\mathbb{B}_E$ whose fixed field, as a pure field, is isomorphic to $\mathbb{R}$, such that E is continuous in the induced topology, and the three above equations are satisfied.

The author announced in [5] the positive answer to the first of the above questions for Zilber fields of cardinality up to the continuum, including $\mathbb{B}$, without the monotonicity clause:

Theorem 1.1. *If K_E is a Zilber field of cardinality $|K| \leq 2^{\aleph_0}$, then there exists has an involution σ on K_E, i.e., there is a field automorphism $\sigma : K \to K$ of order two such that $\sigma \circ E = E \circ \sigma$.*

Moreover, if $K_E = \mathbb{B}$, there is a σ such that $K^\sigma \cong \mathbb{R}$ and $\ker(E) = 2\pi i\mathbb{Z}$.

Here we describe the complete proof of this statement. In order to deduce the theorem, we actually take the opposite route: we start from a given automorphism σ of the field K, and we construct a suitable function E. We prove the following:

Theorem 1.2. *There is a function $E : \mathbb{C} \to \mathbb{C}^\times$ such that $\mathbb{C}_E$ is a Zilber field, $E(\overline{z}) = \overline{E(z)}$ for all $z \in \mathbb{C}$, and $E(2\pi i(p/q)) = e^{2\pi i(p/q)}$ for all $p \in \mathbb{Z}$, $q \in \mathbb{Z}^\times$.*

More generally, let K be an algebraically closed field of, $\sigma : K \to K$ an automorphism of order two, and ω transcendental number in the fixed field K^σ.

If K is uncountable and the order topology of K^σ is second-countable, then there is a function $E : K \to K^\times$ such that K_E is a Zilber field, $\sigma \circ E = E \circ \sigma$ and $\ker(E) = i\omega\mathbb{Z}$.

Note that if the order topology of K^σ is second-countable, then the cardinality of K cannot be greater than $2^{\aleph_0}$. Moreover, for σ to exist in the first place, K must have characteristic 0.

To see that Theorem 1.1 follows from Theorem 1.2 in the uncountable case, it is sufficient to take an uncountable real closed subfield $R \subset \mathbb{R}$ of the right cardinality and apply the theorem to the algebraic closure $\overline{R}$ and the unique non-trivial automorphism of $\overline{R}/R$. By categoricity, all Zilber fields of the same cardinality of R will be isomorphic to $\overline{R}_E$ and will have an involution.

In order to treat (uniformly) also the countable case, we have to use the fact that Zilber fields of the same *exponential transcendence degree* (see [3]) are isomorphic. The uncountable case is recovered by the fact that the cardinality is equal to the degree as soon as it is infinite.

Indeed, by the above argument, we can start with the Zilber field $\mathbb{C}_E (\cong \mathbb{B})$ of cardinality $2^{\aleph_0}$ and with complex conjugation as our σ. If $\{t_j\}_{j<\kappa} \subset \mathbb{R}$ is an exponentially-algebraically independent set of cardinality κ, its exponential-algebraic closure $K' := \mathrm{cl}(\{t_j\})$ and the restriction $E' := E_{\restriction K'}$ yield a Zilber filed $K'_{E'}$ of degree κ. Since cl is $\mathcal{L}_{\omega_1,\omega}$-definable, it is preserved by σ, so we have that $\sigma(\mathrm{cl}(\{t_j\})) = \mathrm{cl}(\{\sigma(t_j)\}) = \mathrm{cl}(\{t_j\})$, hence $\sigma_{\restriction K'}$ is an involution of $K'_{E'}$. Since all Zilber fields of degree κ are isomorphic to $K'_{E'}$, we have found an involution for all of them.

As a corollary of the above arguments, we obtain that there are actually several non-isomorphic involutions on Zilber fields, as we can choose to fill or omit the Dedekind sections over $\mathbb{Q}$ of each t_j (see Theorem 4.1).

On the other hand, our construction has a strong limitation: it produces a function E that is not continuous with respect to the topology induced by σ, even if we restrict to K^σ. Actually, the class of structures (K_E, σ) that we produce is quite strange. The topology induced by σ *is* related to E, but in a rather different way from $\mathbb{C}_{\exp}$ with complex conjugation: we get dense sets of solutions on rotund varieties of depth 0 rather than isolated solutions (see Section 4).

The author would like to thank Jonathan Kirby, who inspired this work, and suggested many corrections, Prof. Alessandro Berarducci, for the numerous suggestions, and Prof. Zannier for the encouraging comments.

2. Definitions and axioms

We recall briefly the basic concepts needed to work with Zilber fields, and the list of their axioms. We also fix some notation and some naming conventions, mostly borrowing from [3]. A more succinct account of the axioms, but with a different notation, can be found in [6].

2.1. **Definitions.** Let us take some notation from Diophantine geometry: we denote by $\mathbb{G}_a$ the *additive* group and by $\mathbb{G}_m$ the *multiplicative* group. In other words, we have $\mathbb{G}_a(K) = (K, +)$ and $\mathbb{G}_m(K) = (K^\times, \cdot)$. We call $\mathbb{G}$ the product $\mathbb{G}_a \times \mathbb{G}_m$, and we denote its group action by $\oplus$. The group $\mathbb{G}$ is a natural environment where to look at points of the form $(z, E(z)) \in \mathbb{G}_a \times \mathbb{G}_m = \mathbb{G}$.

The group $\mathbb{G}$ is naturally a $\mathbb{Z}$-module as an abelian group:

$$\begin{aligned} (\cdot) : \mathbb{Z} \times \mathbb{G} &\to \mathbb{G} \\ m \cdot (z, w) &\mapsto (m \cdot z, w^m). \end{aligned}$$

The action can be naturally generalized to matrices with integer coefficients.

$$\begin{aligned} (\cdot) : \mathcal{M}_{k,n}(\mathbb{Z}) \times \mathbb{G}^n &\to \mathbb{G}^k \\ (m_{i,j})_{i,j} \cdot (z_j, w_j)_j &\mapsto \left(\sum_{j=1}^n m_{i,j} z_j, \prod_{j=1}^n w_j^{m_{i,j}} \right)_i . \end{aligned}$$

Using this notation, we can state the following definition.

Definition 2.1. An irreducible subvariety V of $\mathbb{G}^n$, for some positive integer n, is *rotund* if for all $M \in \mathcal{M}_{n,n}(\mathbb{Z})$ the following inequality holds:

$$\dim M \cdot V \geq \operatorname{rank} M.$$

In the original conventions of [8], a rotund variety is called "ex-normal", and it was later converted to just "normal". However, we preferred the convention of [3] not to risk confusion with the term "normal" from algebraic geometry.

Note that we do not specify the base field over which V is irreducible; it can happen that V is irreducible, but not absolutely irreducible, as it can split into finitely many subvarieties when enlarging the field of definition. The absolutely irreducible components of a rotund variety, i.e., the ones irreducible over the algebraic closure, are still rotund.

Let us call π_a and π_m the projections of $\mathbb{G}$ on its two factors $\mathbb{G}_a$ and $\mathbb{G}_m$ resp.

Definition 2.2. An irreducible subvariety V of $\mathbb{G}^n$, for some integer n, is *absolutely free* if for all non-zero matrices $M \in \mathcal{M}_{n,1}(\mathbb{Z})$ the following holds:

$$\dim \pi_a(M \cdot V) = \dim \pi_m(M \cdot V) = 1.$$

In Zilber's paper [8] there is a relative notion of "freeness". We do not need it here. As above, if V is absolutely free, all of its absolutely irreducible components will be absolutely free.

Absolutely free rotund varieties are to be thought as system of equations in one iteration of E which are compatible with the Schanuel's Property (see below) and are not overdetermined. Indeed, here are their solutions.

Notation 2.3. For any positive integer number n, and for any two given vectors $\overline{z} = (z_1, \ldots, z_n) \in K^n$ and $\overline{w} = (w_1, \ldots, w_n) \in (K^\times)^n$, we denote by $\langle \overline{z}; \overline{w} \rangle$ the 'interleaved' vector $((z_1, w_1), \ldots, (z_n, w_n)) \in \mathbb{G}^n(K)$.

If $\overline{z} = (z_1, \ldots, z_n) \in K^n$, we write $E(\overline{z})$ to denote $(E(z_1), \ldots, E(z_n)) \in (K^\times)^n$.

Definition 2.4. If V is an absolutely free rotund variety $V \subset \mathbb{G}^n$, a vector $\overline{z} \in K^n$ is a *solution* of V if $\langle \overline{z}; E(\overline{z}) \rangle \in V$.

Let us suppose that the absolutely free rotund variety $V \subset \mathbb{G}^n$ is defined over some finite tuple $\overline{c} \in K^{<\omega}$.

Notation 2.5. We write $V(\overline{c})$ to denote a variety V and a finite tuple of parameters $\overline{c}$ such that V is defined over $\overline{c}$.

This notation can also be thought as saying that V is obtained from some $\emptyset$-definable family $V(\overline{x})$ when specializing the parameters to $\overline{c}$.

Definition 2.6. A solution $\overline{z} \in K^n$ is a *generic solution of* $V(\overline{c})$ when the corresponding point $\langle \overline{z}; E(\overline{z}) \rangle \in V$ is generic over $\overline{c}$ in the algebraic sense, i.e., when

$$\operatorname{tr.deg.}_{\overline{c}} \langle \overline{z}; E(\overline{z}) \rangle = \dim V.$$

A set of generic solutions $\mathcal{S}$ of $V(\overline{c})$ is *algebraically independent* if for any finite subset $\{\overline{z}_1, \ldots, \overline{z}_k\} \subset \mathcal{S}$ the following holds:

$$\operatorname{tr.deg.}_{\overline{c}}(\langle \overline{z}_1; E(\overline{z}_1) \rangle, \ldots, \langle \overline{z}_k; E(\overline{z}_k) \rangle) = k \cdot \dim V.$$

A special role is given to the varieties $V \subset \mathbb{G}^n$ such that $\dim V = n$. For convenience, we define the following quantity.

Definition 2.7. The *depth* of a variety $V \subset \mathbb{G}^n$ is $\delta(V) = \dim V - n$.

Hence a variety with $\dim V = n$ has "depth 0". For all rotund varieties, $\delta(V) \geq 0$. The varieties of depth 0 characterize the exponential-algebraic elements, and in some sense, they represent 'finite' exponential-algebraic extensions (see [3]).

Definition 2.8. An absolutely free rotund variety $V \subset \mathbb{G}^n$ is *simple* if for all $M \in \mathcal{M}_{n,n}(\mathbb{Z})$ with $0 < \mathrm{rank} M < n$ the following strict inequality holds:

$$\dim M \cdot V > \mathrm{rank} M.$$

Simple varieties represent "simple" extensions, as in Hrushovski's amalgamation terminology, or in other words extensions without proper exponential-algebraic subextensions. The special case of simple algebraic extensions is represented by the following varieties.

Definition 2.9. An absolutely free rotund variety $V \subset \mathbb{G}^n$ is *perfectly rotund* if it is simple and it has depth 0.

2.2. **Zilber's axioms.** Now that we have given all the relevant definitions, we can list the axioms defining Zilber fields. Let K_E be our structure. We split the axioms into three groups depending on their meaning for $\mathbb{C}_{\exp}$.

Trivial properties of $\mathbb{C}_{\exp}$.

(ACF_0) K is an algebraic closed field of characteristic 0.
(E) E is a homomorphism $E : (K, +) \to (K^\times, \cdot)$.
(LOG) E is surjective (every element has a logarithm).
(STD) the kernel is a cyclic group, i.e., $\ker E = \omega\mathbb{Z}$ for some $\omega \in K^\times$.

Axioms conjecturally true on $\mathbb{C}_{\exp}$.

(SP) *Schanuel's Property*: for every finite tuple $\overline{z} = (z_1, \ldots, z_n) \in K$ such that $z_1, \ldots, z_n$ are linearly independent over $\mathbb{Q}$,

$$\mathrm{tr.deg.}_{\mathbb{Q}}\langle \overline{z}; E(\overline{z})\rangle = \mathrm{tr.deg.}_{\mathbb{Q}}(z_1, \ldots, z_n, E(z_1), \ldots, E(z_n)) \geq n.$$

(SEC) *Strong Exponential-algebraic Closure*: for every absolutely free rotund variety $V \subset \mathbb{G}^n$ over K, and every finite tuple $\overline{c} \in K^{<\omega}$ such that V is defined over $\overline{c}$, $V(\overline{c})$ has a generic solution $\overline{z} \in K^n$.

A non-trivial property of $\mathbb{C}_{\exp}$ [8, Lemma 5.12].

(CCP) *Countable Closure Property*: for every absolutely free rotund variety $V \subset \mathbb{G}^n$ over K of depth 0, and every finite tuple $\overline{c} \in K^{<\omega}$ such that V is defined over $\overline{c}$, the set of the generic solutions of $V(\overline{c})$ is at most countable.

If K_E satisfies the above seven axioms, then we say that K_E is a Zilber field. By Zilber's theorem [8], if K_E is uncountable, its isomorphism type is completely determined by its cardinality, and in general it is determined by its exponential transcendence degree. The one of cardinality $2^{\aleph_0}$ is called $\mathbb{B}$, $\mathbb{B}_E$ or $\mathbb{B}_{\mathrm{ex}}$, and it is sometimes called *the* Zilber field, as it is the one conjecturally isomorphic to $\mathbb{C}_{\exp}$.

Some authors also add the axiom "K_E has infinite exponential transcendence degree", so that also the countable model is determined just by the cardinality, but we do not need this extra assumption here.

3. The construction

As anticipated in the introduction, the proof of Theorem 1.2 is obtained with an explicit construction. Our starting data are a field K, an involution σ of K and some transcendental ω in the fixed field K^σ. Our result is a function E such that K_E is a Zilber field, $\sigma \circ E = E \circ \sigma$ and $\ker(E) = i\omega\mathbb{Z}$. We describe here the procedure, and the proof that the resulting K_E has the desired properties will be given throughout the rest of the paper.

The idea is to define E inductively by back-and-forth: at one step, we define the function on a new element of K, at another we define it so that a new element of

$K^\times$ appears in the image, and in the meanwhile we add solutions to each rotund variety (in a sensible way).

At the various stages of the construction we shall deal with *partial* functions E_j. Thus, it shall be convenient to speak of *partial E-fields*, which are the structures K_E satisfying the following 'partial version' of the axiom (E).

(E-par) E is a homomorphism $E : (D, +) \to (K^\times, \cdot)$, where D is a divisible subgroup of K.

We stress the fact that in (E-par) we require the domain of E to be divisible; in other words, it is a $\mathbb{Q}$-linear vector space. Note that we are also implicitly assuming that the field has characteristic 0. When the domain D is the whole K, we say that K_E is just a (global) *E-field*.

In order to have $\sigma \circ E = E \circ \sigma$ at each stage, we use a rather easy observation. Let us copy the usual notation for $\mathbb{C}$ and $\mathbb{R}$ to our case. We denote by R the fixed field K^σ, which is a real closed field; if i is a square root of -1, we have $K = R(i)$.

We define:

(1) the *real part* of $z \in K$ as $\Re(z) := \frac{z+\sigma(z)}{2}$;
(2) the *imaginary part* of $z \in K$ as $\Im(z) := \frac{z-\sigma(z)}{2i}$;
(3) the *modulus* of $z \in K^\times$ as $|z| := \sqrt{z \cdot \sigma(z)}$;
(4) the *phase* of $z \in K^\times$ as $\Theta(z) := \frac{z}{|z|}$ (not so usual after all).

The former two are the additive decomposition of a number of K over R, the latter are its multiplicative decomposition. The image of the function Θ is the 'unit circle', and it will be denoted by $\mathbb{S}^1(K) = \{z \in K^\times : |z| = 1\}$.

Using this description, it is quite easy to see the following.

Proposition 3.1. *Let K_E be a partial E-field, and $\sigma : K \to K$ be a field automorphism of order two. Then $\sigma \circ E = E \circ \sigma$ if and only if the following three conditions are satisfied:*

(1) $\sigma(\mathrm{dom}(E)) = \mathrm{dom}(E)$*;*
(2) $E(R) \subset R_{>0}$*;*
(3) $E(iR) \subset \mathbb{S}^1(K)$*;*

Proof. If $\sigma \circ E = E \circ \sigma$, it is clear that $\sigma(\mathrm{dom}(E)) = \mathrm{dom}(E)$. For all $x \in R$ we have $\sigma(E(x)) = E(x)$, which implies $E(x) \in R$, and since $E(x) = E\left(\frac{x}{2}\right)^2$, it is actually $E(x) \in R_{>0}$; moreover, for all $y \in R$ we have $\sigma(E(iy)) = E(-iy) = E(iy)^{-1}$, i.e., $|E(iy)| = \sqrt{\sigma(E(iy))E(iy)} = 1$.

On the other hand, suppose that the three conditions are satisfied. We have then that for all $x, y \in R$, $\sigma(E(x)) = E(x)$ and $\sigma(E(iy)) = E(iy)^{-1}$. Since any $z \in K$ can be written uniquely as $x + iy$ with $x, y \in R$, and if E is defined over z, by the first condition it is also defined over $x = \Re(z)$ and $y = \Im(z)$, we have

$$\sigma(E(z)) = \sigma(E(x))\sigma(E(iy)) = E(x)E(iy)^{-1} = E(x - iy) = E(\sigma(z)). \qquad \square$$

Hence, in our back-and-forth construction, every time we define the function on a new z linearly independent from the current domain, it shall be sufficient to make sure that either $z \in R$ or that $z \in iR$, and that we define the new values according to the above restrictions.

To begin, let $(\zeta_q)_{q \in \mathbb{N}^\times}$ be a coherent system of roots of unity (i.e., such that $\zeta_{pq}^p = \zeta_q$). We start with the function E_{-1} defined by $E_{-1}(i\frac{p}{q}\omega) := \zeta_q^p$, with domain $\mathrm{dom}(E_{-1}) = i\omega\mathbb{Q}$, and we proceed by transfinite induction.

Let us enumerate the relevant objects:

(1) let $\{\alpha_j\}_{j<|K|}$ be an enumeration of $R \cup iR$;

(2) let $\{\beta_j\}_{j<|K|}$ be an enumeration of $R_{>0} \cup \mathbb{S}^1(K)$;
(3) let $\{V_j\}_{j<|K|}$ be an enumeration of all the simple varieties over K.

The construction itself is based on a certain number of basic 'operation' that we use to extend the partial exponential functions.

In each of the operations, we take a partial E-field K_E such that $\sigma \circ E = E \circ \sigma$, and we extend E to a new function E' with the same properties. We denote by D the domain of E, and by F the field generated by D and $E(D)$. We always assume that $|F| < |K|$.

DOMAIN: We start with a given $\alpha \in R \cup iR$. If $\alpha \in D$, we define $E' := E$, otherwise we do the following.
If $\alpha \in R$, we choose a $\beta \in R_{>0} \setminus \operatorname{acl}(F \cup \{\alpha\})$ and we let $\beta^{1/q}$ be its *positive* roots; if $\alpha \in iR$, we choose a $\beta \in \mathbb{S}^1(K) \setminus \operatorname{acl}(F \cup \{\alpha\})$ and we let $\beta^{1/q}$ be some coherent system of roots.
We define $E'(z + \frac{p}{q}\alpha) := E(z) \cdot \beta^{p/q}$ for all $z \in D$ and $p \in \mathbb{Z}, q \in \mathbb{N}^\times$.

IMAGE: We start with a given $\beta \in R_{>0} \cup \mathbb{S}^1(K)$. If $\beta \in E(D)$, we define $E' := E$, otherwise we do the following.
If $\beta \in R_{>0}$, we choose an $\alpha \in R \setminus \operatorname{acl}(F \cup \{\beta\})$ and we let $\beta^{1/q}$ to be the *positive* roots of β; if $\beta \in \mathbb{S}^1(K)$, we choose an $\alpha \in iR \setminus \operatorname{acl}(F \cup \{\beta\})$ and we let $\beta^{1/q}$ be some coherent system of roots.
We define $E'(z + \frac{p}{q}\alpha) := E(z) \cdot \beta^{p/q}$ for all $z \in D$ and $p \in \mathbb{Z}, q \in \mathbb{N}^\times$.

These operations are used to guarantee that the final function E is surjective and defined everywhere. We also want to verify (SEC), so we use a special operation to add solutions to rotund varieties. However, for reasons that will be clear later, we do this in a rather complicated way. Let us state the following technical definition.

Definition 3.2. Let V be an absolutely irreducible variety. We call the *family $\mathcal{R}(V)$ of the roots of V* the family of all the absolutely irreducible varieties W such that for some $p, q \in \mathbb{Z}^\times$ we have $q \cdot W = p \cdot V$.

Instead of taking a variety V and adding solutions to it, we take all the varieties in the family $\mathcal{R}(V)$ and we add solutions to all of them at once. Moreover, we require the new solutions to be *dense* in the order topology.

SOLUTIONS: We start with the family $\mathcal{R}(V)$ associated to an absolutely irreducible variety V, such that for some finite $\overline{c} \subset D$ closed under σ, all the varieties $W \in \mathcal{R}(V)$ are defined over $\operatorname{acl}(\overline{c}) \cap D$. If every $W \in \mathcal{R}(V)$ contains a dense algebraically independent set of solutions over $\operatorname{acl}(\overline{c})$, we define $E' := E$. Otherwise we do the following.
Let $\mathcal{R}(V)$ be enumerated as $(W_k)_{k<\omega}$, and let $E_{0,0} := E$. We define by double induction on $k, l < \omega$ some new temporary functions $E_{k,l}$.
At step $(k, 0)$ we are given the function $E_{k,0}$. Let $\{U_l\}_{l<\omega}$ be an enumeration of a countable base for the order topology on W_k. At the step (k, l), we take a point $((\alpha_1 + i\gamma_1, \beta_1 \cdot \delta_1), \dots, (\alpha_n + i\gamma_n, \beta_n \cdot \delta_n)) \in U_l \subset r(W_k)$ with the following properties:

$$\begin{gathered} \alpha_j, \gamma_j \in R,\ \beta_j \in R_{>0},\ \delta_j \in \mathbb{S}^1(K) \quad \text{for } 1 \leq j \leq n \\ \operatorname{tr.deg}_{\cdot\overline{c},\operatorname{dom}(E_{k,l}),\operatorname{im}(E_{k,l})}(\alpha_1, \gamma_1, \beta_1, \delta_1, \dots) = 2\dim V. \end{gathered}$$

We fix the positive roots $\beta_j^{1/q}$ of β_j and an arbitrary system of roots $\delta_j^{1/q}$, and we define

$$E_{k,l+1}\left(z + \frac{p_1}{q_1}\alpha_1 + i\frac{p_1'}{q_1'}\gamma_1 + \dots\right) := E_{k,l}(z) \cdot \beta_1^{p_1/q_1} \delta_1^{p_1'/q_1'} \cdot \dots .$$

We define then $E_{k+1,0} := \bigcup_{l<\omega} E_{k,l}$.
At the end, we define $E' := \bigcup_{k<\omega} E_{k,0}$.

These are the *finite* operations. There is only one non-finite operation. Let $(E_k)_{k<j}$ be an increasing sequence of partial exponential functions.

LIMIT: We define $E' := \bigcup_{k<j} E_k$.

The actual construction follows.

(1) If j is a successor ordinal (if $j = 0$, we say that j is the successor of -1) we do the following:
   (a) We apply DOMAIN to α_j and E_j to obtain $E_j^{(1)}$.
   (b) We apply IMAGE to β_j and $E_j^{(1)}$ to obtain $E_j^{(2)}$.
   (c) We take the variety V_j and consider the family $\mathcal{R}(V_j)$. Let $\overline{c}$ be a finite set of parameters closed under σ such that all the varieties in $\mathcal{R}(V_j)$ are defined over $\mathrm{acl}(\overline{c})$.
   Let us enumerate $(\mathrm{acl}(\overline{c})^\sigma \cup i\mathrm{acl}(\overline{c})^\sigma)$ as $(c_k)_{k<\omega}$. We define inductively a sequence of functions $(E^k)_{k<\omega}$ in this way: E^0 is the function $E_j^{(2)}$, and the function E^{k+1} is obtained from E^k applying DOMAIN to c_k. After the induction, we apply LIMIT to the sequence $(E^k)_{k<\omega}$ to obtain the function $E_j^{(3)}$.
   (d) At last, we apply SOLUTIONS to the family $\mathcal{R}(V_j)$ and the function $E_j^{(3)}$. The function resulting from this operation is E_{j+1}.

(2) If j is a limit ordinal we apply LIMIT to the sequence $(E_k)_{k<j}$ to obtain the function E_j.

We claim that $E_{|K|}$ is the desired function.

4. An (involuntary) restriction on σ

Before entering the details of the proof of Theorem 1.2, we wish to comment the fact that the resulting exponential function behaves rather badly with respect to the topology induced by σ, and quite differently from the classical case $\mathbb{C}_{\exp}$.

Indeed, we can easily describe a restricted class of involutions containing the ones obtained with our method. Let (K_E, σ) be a structure where K_E is a Zilber field and σ is an involution of K_E. Consider the following axioms:

(ZIL) K_E is a Zilber field;

(INV) σ is an automorphism of order two;

(DEN) for every absolutely free rotund variety $V \subset \mathbb{G}^n$ over K, every finite tuple $\overline{c} \in K^{<\omega}$ such that V is defined over $\overline{c}$, and every subset $U \subset V$ open w.r.t. the order topology of K^σ, there is a generic solution $\overline{z} \in K^n$ of $V(\overline{c})$ such that $\langle \overline{z}; E(\overline{z})\rangle \in U$.

The last axioms means that for each absolutely free rotund variety $V(\overline{c})$ the set of its generic solutions is dense in the order topology. In some sense, we are saying that E is not only random with respect to the field structure, but also with respect to the order structure. It can be expressed by a first order formula with a slight modification of axiom (SEC).

Our proof shows explicitly the existence of many models in the above class.

Theorem 4.1. *For each cardinal $0 < \kappa \leq 2^{\aleph_0}$, there are $2^{\aleph_0+\kappa}$ pairwise non-isomorphic models of the axioms (ZIL), (INV), (DEN) of dimension κ. There is at least one model of dimension 0.*

It is a direct consequence of our construction that there is one such model built on $\mathbb{C}$ and complex conjugation; the existence of the other models can be deduced as we did for Theorem 1.1. If $\{t_j\}_{j<2^{\aleph_0}}$ is a maximal exponentially-algebraically independent subset of $\mathbb{R}$, then it is sufficient to choose κ elements of $\{t_j\}$ and take their exponential algebraic closure; it is easy to verify that the closure still satisfies

(DEN). As the Dedekind sections of the elements that get left out are *not* filled when taking the closure, we obtain 2^κ non-isomorphic real closed fields, hence as many non-isomorphic models, when κ is infinite, $2^{\aleph_0}$ when κ is finite, and at least one of dimension 0.

However, our method does not say anything about models where the axiom (DEN) is not true. In particular, even if $\mathbb{C}_{\exp}$ is a Zilber field, and σ is the classical complex conjugation, $(\mathbb{C}_{\exp}, \sigma)$ cannot be a result of our construction.

Moreover, (CCP) and (DEN) imply that the topology must be separable, hence the cardinality of K is forced to be at most $2^{\aleph_0}$.

5. Some facts about Zilber fields

In order to prove that the resulting E-field $K_{E_{|K|}}$ of Section 3 is a Zilber field, we need to check that each of the axioms listed in Section 2 is true. Using some known properties and tools of Zilber fields, we can reduce a bit the complexity of this problem.

Here we recall two equivalent, but simpler formulations of the axioms (SEC) and (CCP), and some properties of the predimension of Zilber fields that helps in verifying (SP).

5.1. **Equivalent formulations.** The axioms (SEC) and (CCP) can be verified just using simple and perfectly rotund varieties rather than all rotund varieties. This is the reason why it is sufficient to use simple varieties in step 1d. Moreover, at least for (SEC) the parameters defining the varieties are not important.

Fact 5.1. *Let K_E be a partial E-field. (SEC) holds on K_E if and only if the following holds:*

(SEC$_1$) *for any absolutely irreducible simple variety V defined over* some *finite $\overline{c}$, $V(\overline{c})$ has an infinite set of algebraically independent solutions.*

Fact 5.2. *Let K_E be a partial E-field. (CCP) holds on K_E if and only if the following holds:*

(CCP$_1$) *for any perfectly rotund variety V, and for any finite $\overline{c}$ such that V is defined over $\overline{c}$, $V(\overline{c})$ has at most countably many generic solutions.*

Hence, it is sufficient to verify (SEC$_1$) and (CCP$_1$) instead of their full versions. We use the following fact.

Proposition 5.3. *Let V be an absolutely free rotund variety. Let $\overline{c}$ and $\overline{d}$ be two finite tuples such that V is defined both over $\overline{c}$ and over $\overline{d}$.*

If $\mathcal{S}$ is a set of algebraically independent solutions of $V(\overline{c})$, then $\mathcal{S}$, up to removing a finite set, is an algebraically independent set of solutions of $V(\overline{d})$.

Proof. For each finite subset $\mathcal{S}' \subset \mathcal{S}$, let $\Delta(\mathcal{S})$ be the following quantity:

$$\Delta(\mathcal{S}') := \text{tr.deg.}_{\overline{c}}(\mathcal{S}') - \text{tr.deg.}_{\overline{d}}(\mathcal{S}') = \dim V \cdot |\mathcal{S}'| - \text{tr.deg.}_{\overline{d}}(\mathcal{S}').$$

Δ measures how far is $\mathcal{S}'$ from being algebraically independent over $\overline{d}$. First of all, we claim that $\Delta(\mathcal{S}')$ is bounded from above. Indeed,

$$\text{tr.deg.}_{\overline{d}}(\mathcal{S}') \geq \text{tr.deg.}_{\overline{c},\overline{d}}(\mathcal{S}') \geq \text{tr.deg.}_{\overline{c}}(\mathcal{S}') - \text{tr.deg.}_{\overline{c}}(\overline{d}),$$

and after shuffling the terms, $\Delta(\mathcal{S}') \leq \text{tr.deg.}_{\overline{c}}(\overline{d})$. Moreover, Δ is clearly increasing.

Now let $\mathcal{S}_0$ be a finite set such that $\Delta(\mathcal{S}_0)$ is maximum. We claim that $\mathcal{S} \setminus \mathcal{S}_0$ is algebraically independent. Let us consider a finite subset $\mathcal{S}' \subset \mathcal{S} \setminus \mathcal{S}_0$; since the function Δ is increasing, we have

$$\begin{aligned}\dim V \cdot (|\mathcal{S}'| + |\mathcal{S}_0|) - \text{tr.deg.}_{\overline{d}}(\mathcal{S}' \cup \mathcal{S}_0) = \Delta(\mathcal{S}' \cup \mathcal{S}_0) = \\ = \Delta(\mathcal{S}_0) = \dim V \cdot |\mathcal{S}_0| - \text{tr.deg.}_{\overline{d}}(\mathcal{S}_0).\end{aligned}$$

This implies that

$$\dim V \cdot |\mathcal{S}'| \geq \mathrm{tr.deg.}_{\overline{d}}(\mathcal{S}') \geq \mathrm{tr.deg.}_{\overline{d},\mathcal{S}_0}(\mathcal{S}') = \dim V \cdot |\mathcal{S}'|,$$

as desired. □

Proof of Facts 5.1 and 5.2. One direction is trivial for both statements, so let us see the other direction.

Let V be an absolutely free rotund variety over $\overline{c}$. By adding some elements of $\mathrm{acl}(\overline{c})$ to $\overline{c}$, we find that V splits into a finite union of conjugate absolutely irreducible varieties. In particular, all of them are absolutely free and rotund. If we verify that (SEC) and (CCP) hold when specialized in each of these components, then (SEC) and (CCP) are also true when specialized in V. Hence, we may assume that V is absolutely irreducible.

We proceed by induction on $n = \dim(V)$. If V is simple, and (SEC_1) is true, then V has infinitely many algebraically independent solutions over some set of parameters $\overline{d}$, and by Proposition 5.3, up to removing a finite number of them, they are also algebraically independent over $\overline{c}$. If V is perfectly rotund, and (CCP_1) is true, there are at most countably many generic solutions.

Now, let us suppose that V is not simple, and that we have proved the conclusions for all the varieties of dimension smaller than V. Let $z_1, w_1, \dots, z_n, w_n$ be the coordinate functions of V.

Let M be a matrix such that $0 < k = \mathrm{rank} M < n$ and $\dim M \cdot V = \mathrm{rank} M$. Using a suitable square invertible matrix, we may assume that M is the projection of V over the coordinates $z_1, w_1, \dots, z_k, w_k$.

Let N be a matrix in $\mathcal{M}_{h,n-k}(\mathbb{Z})$ of maximum rank, with $h \leq n-k$. By rotundity, we have

$$\mathrm{tr.deg.}_{\overline{c}}\left(\begin{pmatrix} M & 0 \\ 0 & N \end{pmatrix} \cdot (z_1, w_1, \dots, z_n, w_n)\right) \geq k + h.$$

But since $\dim M \cdot V = k$, this means

$$\mathrm{tr.deg.}_{\overline{c}, z_1, \dots, z_k, w_1, \dots, w_k}(N \cdot (z_{k+1}, w_{k+1}, \dots, z_n, w_n)) \geq h = \mathrm{rank} N.$$

This means that whenever we specialize the first $2k$ coordinates to a generic solution of $M \cdot V$, the remaining coordinates describe a *rotund* variety of smaller dimension.

The projection $M \cdot V$ is a rotund variety of depth 0. If (SEC_1) is true, by inductive hypothesis it contains infinitely many algebraically independent solution. If (CCP_1) is true, by inductive hypothesis it contains no more than countably many generic solutions.

Now, let us suppose that $\tilde{z} = (\tilde{z}_1, \dots, \tilde{z}_k)$ is a solution of $M \cdot V$ (if there is one). If we specialize the variables $z_1, w_1, \dots, z_k, w_k$ to $\tilde{z}_1, E(\tilde{z}_1), \dots, \tilde{z}_k, E(\tilde{z}_k)$, and we project onto the last $2(n-k)$ coordinates, we obtain a new variety $\tilde{V}(\overline{c}, \tilde{z}, E(\tilde{z}))$.

But $\tilde{V}$ is a *rotund* variety of dimension smaller than V. If (SEC_1) is true, by inductive hypothesis it must have infinitely many algebraically independent solutions, and combining all the generic solutions $\tilde{z}$ of $M \cdot V$ and all the solutions of the corresponding $\tilde{V}(\overline{c}, \tilde{z}, E(\tilde{z}))$, we obtain that there are infinitely many algebraically independent solutions in $V(\overline{c})$.

On the other hand, if V has depth 0, then $\tilde{V}$ has also depth 0. If (CCP_1) is true, by inductive hypothesis $M \cdot V(\overline{c})$ has at most countably many generic solutions $\overline{z}$ over $\overline{c}$, and for each of them, $\tilde{V}(\overline{c}, \tilde{z}, E(\tilde{z}))$ has at most countably many generic solutions; hence, $V(\overline{c})$ contains at most countably many generic solutions.

Hence, (SEC_1) implies (SEC) and (CCP_1) implies (CCP). □

5.2. **Predimension.** The axiom (SP) can be interpreted as stating that a certain quantity is always positive, and in the context of Hrushovski's amalgamation, this quantity works as a predimension on K_E. The predimension is particularly useful when dealing with exponential fields, even when (SP) is not true, and it is a crucial tool in Zilber's proof of categoricity of Zilber fields. In our case, we actively use its machinery to verify that (SP) holds on $K_{E_{|K|}}$.

Let K_E be a partial E-field. Given a set X contained in the domain of E, we denote by $E(X)$ the image of the elements of X through E.

Definition 5.4. Let $X \subset \mathrm{dom}(E)$ be a finite set. The *predimension* of X is the quantity

$$\delta(X) = \mathrm{tr.deg.}_{\mathbb{Q}}(X \cup E(X)) - \mathrm{lin.d.}_{\mathbb{Q}}(X).$$

If X is a finite subset of K, and Y an arbitrary subset of K such that E is defined on X and Y, we define

$$\delta(X/Y) := \mathrm{tr.deg.}_{\mathbb{Q}}(X \cup E(X)/Y \cup E(Y)) - \mathrm{lin.d.}_{\mathbb{Q}}(X/Y).$$

In these definitions, $\mathrm{tr.deg.}_{\mathbb{Q}}(X)$ stays for the transcendence degree of X over the base field $\mathbb{Q}$, while $\mathrm{lin.d.}_{\mathbb{Q}}(X)$ means the $\mathbb{Q}$-linear dimension of X. Instead, $\mathrm{tr.deg.}_{\mathbb{Q}}(X/Y)$ is the transcendence degree of X over $\mathbb{Q}(Y)$, and $\mathrm{lin.d.}_{\mathbb{Q}}(X/Y)$ is the linear dimension of X over the $\mathbb{Q}$-linear span of Y. In order to reduce the size of the formulas, we will often write also $\mathrm{tr.deg.}_Y(X)$ to denote the transcendence degree of X over Y.

With this notation, (SP) is equivalent to $\delta(X) \geq 0$ for all X.

Remark 5.5. The definition of predimension is slightly different from [8], as we calculate it *only on the domain of E*. We are again following [3], as it greatly simplifies the discussion.

Definition 5.6. Let $K_E \subset K'_{E'}$ be two partial E-fields. Let δ and δ' the two respective predimension functions.

We say that $K_E \leq K'_{E'}$, or that K_E is *strongly embedded* in $K'_{E'}$, if for each finite $X \subset \mathrm{dom}(E')$ we have $\delta'(X/\mathrm{dom}(E)) \geq 0$.

If $X \subset \mathrm{dom}(E)$ we say that X is *strong* in K_E, $X \leq K_E$, if $K_{E_{\restriction \mathrm{span}_{\mathbb{Q}}(X)}} \leq K_E$.

Some facts about predimensions, and in particular their relationship with rotund varieties are useful tools in proofs. See [3] for reference.

Fact 5.7. *The axiom (SP) holds on K_E if and only if $\{0\} \leq K_E$.*

If $K_E \leq K'_{E'} \leq K''_{E''}$, then $K_E \leq K''_{E''}$. In particular, if K_E satisfies (SP) and $K_E \leq K'_{E'}$, then $K'_{E'}$ satisfies (SP).

Fact 5.8. *Let K_E a partial E-field satisfying (SP). Then for all finite $X \subset \mathrm{dom}(E)$ there is a finite $Y \subset \mathrm{dom}(E)$ such that $XY \leq K_E$.*

For the last statement, it is sufficient that K_E satisfies an "almost Schanuel's Property" stating that there is a k such that $\delta(Z) \geq k$ for all Z. This implies that $\delta(XY)$ attains a minimum as Y varies, proving the statement (see again [3]).

Let V be an absolutely free rotund variety over K, and let $((z_1, w_1), \dots, (z_n, w_n))$ be a generic point of V over K into some field extension K'.

Fact 5.9. *If we extend linearly E to a function E' by defining $E'(\frac{p}{q} z_i) = w_i^{p/q}$, then the new function is well defined and $K_E \leq K'_{E'}$. Moreover,* $\ker(E) = \ker(E')$.

6. Preserving CCP

The most difficult axiom to verify on the E-field $K_{E_{|K|}}$ of Section 3 is (CCP), even in its weaker form (CCP_1). In this section we show that (CCP) is preserved

by the finite operations, i.e., if (CCP) holds at some stage of our construction, it holds after the application of one of the finite operations, and in particular it holds also for the successive stage.

More precisely, we claim that if K_E satisfies (CCP), and we extend linearly E to E' by defining E' on some finite, or even countable, set of elements that are $\mathbb{Q}$-linearly independent over $\mathrm{dom}(E)$, then also $K_{E'}$ satisfies (CCP). This kind of fact is already known, but it has not been stated in literature, and since it is quite important for our constructions, we describe it here in full details.

We prove it in two steps. First, we show that there is an equivalent formulation of (CCP) which is even simpler than (CCP_1), under the assumption that (SP) holds; then, using the simplified formulation, we prove that (CCP) is preserved if we extend the function E on a not too large set.

Proposition 6.1. *Let K_E be a partial EA-field satisfying (SP). Then axiom (CCP) is equivalent to*

(CCP_2) *for any perfectly rotund variety V defined over* $\mathrm{dom}(E)$*, and for any finite tuple $\overline{c} \subset \mathrm{dom}(E)$ such that V is defined over $\overline{c}$, there are at most countably many generic solutions of $V(\overline{c})$.*

Proof. The left-to-right direction is clear. Let us prove the other direction.

Let us suppose that K_E satisfies (CCP_2). Let $X(\overline{c}) \subset \mathbb{G}^n$ be a perfectly rotund variety. Without loss of generality, we may assume that $\overline{c}$ is of the form $\overline{c}_0\overline{c}_1$, with $\overline{c}_0 \subset \mathrm{dom}(E)$ and $\overline{c}_1$ $\mathbb{Q}$-linearly independent from $\mathrm{dom}(E)$.

Let $\overline{d}$ be a finite subset of $\mathrm{dom}(E)$ such that

(1) $\overline{c}_0\overline{d} \leq K_E$;
(2) $\mathrm{tr.deg.}_{\langle \overline{c}_0\overline{d}; E(\overline{c}_0\overline{d})\rangle}(\overline{c}_1) = \mathrm{tr.deg.}_{\mathrm{dom}(E),\mathrm{im}(E)}(\overline{c}_1)$.

It exists by Fact 5.8.

Now, let us take a generic solution $\overline{z}$ of $X(\overline{c})$. There is an invertible matrix M with coefficients in $\mathbb{Z}$ such that $M \cdot \overline{z}$ is of the form $\overline{z}_0\overline{z}_1$, with $\overline{z}_0 \subset \mathrm{span}_{\mathbb{Q}}(\overline{c}_0\overline{d})$ and $\overline{z}_1$ $\mathbb{Q}$-linearly independent from $\mathrm{span}_{\mathbb{Q}}(\overline{c}_0\overline{d})$.

By hypothesis, $\overline{c}_0\overline{d} \leq K_E$, so for any matrix N with integer coefficients:

$$\mathrm{tr.deg.}_{\langle \overline{c}_0\overline{d}; E(\overline{c}_0\overline{d})\rangle}\langle N \cdot \overline{z}_1; E(N \cdot \overline{z}_1)\rangle \geq \mathrm{rank} N.$$

Moreover, since $\overline{z}_0\overline{z}_1$ is a generic point of $M \cdot X(\overline{c})$, which is a perfectly rotund variety defined over $\overline{c}$, we have

$$\mathrm{tr.deg.}_{\overline{c}\langle \overline{z}_0; E(\overline{z}_0)\rangle}\langle \overline{z}_1; E(\overline{z}_1)\rangle \leq |\overline{z}_1|.$$

Clearly, since $\overline{z}_0 \subset \mathrm{span}_{\mathbb{Q}}(\overline{c}_0\overline{d})$, this implies

$$\mathrm{tr.deg.}_{\overline{c}_1\langle \overline{c}_0\overline{d}; E(\overline{c}_0\overline{d})\rangle}\langle \overline{z}_1; E(\overline{z}_1)\rangle \leq |\overline{z}_1|.$$

In particular, since $\mathrm{tr.deg.}_{\langle \overline{c}_0\overline{d}\overline{z}_1; E(\overline{c}_0\overline{d}\overline{z}_1)\rangle}(\overline{c}_1) = \mathrm{tr.deg.}_{\langle \overline{c}_0\overline{d}; E(\overline{c}_0\overline{d})\rangle}(\overline{c}_1)$, we have

$$|\overline{z}_1| \leq \mathrm{tr.deg.}_{\langle \overline{c}_0\overline{d}; E(\overline{c}_0\overline{d})\rangle}\langle \overline{z}_1; E(\overline{z}_1)\rangle = \mathrm{tr.deg.}_{\overline{c}_1\langle \overline{c}_0\overline{d}; E(\overline{c}_0\overline{d})\rangle}\langle \overline{z}_1; E(\overline{z}_1)\rangle \leq |\overline{z}_1|.$$

This implies that $\overline{z}_1$ is a generic solution of a perfectly rotund variety defined over $\overline{c}_0\overline{d}$. As there are countably many such varieties, and K_E satisfies (CCP_2), then there are at most countably many $\overline{z}_1$'s.

To summarize the result, we have

$$\overline{z} = M^{-1}(\overline{z}_0\overline{z}_1).$$

Since there are at most countably many matrices M, at most countably many $\overline{z}_0 \subset \mathrm{span}_{\mathbb{Q}}(\overline{c}_0\overline{d})$ and at most countably many $\overline{z}_1$'s, then there are at most countably many $\overline{z}$. In particular, K_E satisfies (CCP). $\square$

Note that this also explicitly shows what one expects: (CCP) really depends only on E and not on the base field K.

With a very similar argument we obtain our claimed result.

Lemma 6.2. *Let $K_E \subset K'_{E'}$ be two partial E-field satisfying (SP).*

If $\mathrm{dom}(E') = \mathrm{span}_{\mathbb{Q}}(\mathrm{dom}(E) \cup B)$ for some finite or countable $B \subset K'$, then K_E satisfies (CCP) if and only if $K'_{E'}$ does.

Proof. Clearly, if $K'_{E'}$ satisfies (CCP), then K_E does too. For the other direction, let us suppose that K_E satisfies (CCP).

By Proposition 6.1, it is sufficient to prove that $K'_{E'}$ satisfies (CCP_2). Moreover, we may assume that $K = K'$.

Let $X(\overline{c})$ be a perfectly rotund variety, with $\overline{c} \subset \mathrm{dom}(E')$.

Let us take a generic solution of $X(\overline{c})$; by assumptions, it can be written uniquely as $\overline{z}+M\cdot\overline{b}$, with $\overline{z} \subset \mathrm{dom}(E)$, $\overline{b}$ a finite subset of B and M a matrix with coefficients in $\mathbb{Q}$. We claim that given M and $\overline{b}$, there are at most countably many $\overline{z}$'s such that $\overline{z} + M \cdot \overline{b}$ is a generic solution of $X(\overline{c})$.

Let $\overline{d}$ be a finite subset of $\mathrm{dom}(E')$ such that $\overline{b}\overline{c}\overline{d} \leq K'_{E'}$.

There is an invertible matrix N with coefficients in $\mathbb{Z}$ such that $N \cdot \overline{z}$ is of the form $\overline{z}_0\overline{z}_1$, with $\overline{z}_0 \subset \mathrm{span}_{\mathbb{Q}}(\overline{b}\overline{c}\overline{d})$ and $\overline{z}_1$ $\mathbb{Q}$-linearly independent from $\mathrm{span}_{\mathbb{Q}}(\overline{b}\overline{c}\overline{d})$. Thus $(N\cdot\overline{z}+N\cdot M\cdot\overline{b})$ is a generic solution of $N \cdot X(\overline{c})$, which is again a perfectly rotund variety defined over $\overline{c}$. For the sake of notation, let $\overline{b}_0\overline{b}_1$ be the splitting of $N \cdot M \cdot \overline{b}$ corresponding to $\overline{z}_0\overline{z}_1$.

By the hypothesis, $\overline{b}\overline{c}\overline{d} \leq K'_{E'}$, so for any matrix P with integer coefficients

$$\mathrm{tr.deg.}_{\langle \overline{b}\overline{c}\overline{d}; E(\overline{b}\overline{c}\overline{d})\rangle} \langle P\cdot\overline{z}_1; E(P\cdot\overline{z}_1)\rangle \geq \mathrm{rank}P.$$

Moreover, since $\overline{z}_0\overline{z}_1 + \overline{b}_0\overline{b}_1$ is a generic solution of $N \cdot X(\overline{c})$, we have

$$\mathrm{tr.deg.}_{\overline{c}\langle \overline{z}_0+\overline{b}_0; E(\overline{z}_0+\overline{b}_0)\rangle} \langle \overline{z}_1+\overline{b}_1; E(\overline{z}_1+\overline{b}_1)\rangle \leq |\overline{z}_1|.$$

Clearly, since $\overline{z}_0 \subset \mathrm{span}_{\mathbb{Q}}(\overline{b}\overline{c}\overline{d})$, this implies

$$\mathrm{tr.deg.}_{\langle \overline{b}\overline{c}\overline{d}; E(\overline{b}\overline{c}\overline{d})\rangle} \langle \overline{z}_1; E(\overline{z}_1)\rangle \leq |\overline{z}_1|.$$

In particular, we must have

$$|\overline{z}_1| \leq \mathrm{tr.deg.}_{\langle \overline{b}\overline{c}\overline{d}; E(\overline{b}\overline{c}\overline{d})\rangle} \langle \overline{z}_1; E(\overline{z}_1)\rangle \leq |\overline{z}_1|.$$

Hence $\overline{z}_1$ is a generic solution of some perfectly rotund variety defined over $\overline{b}\overline{c}\overline{d}$.

To summarize the result, we have obtained that the generic solutions of $X(\overline{c})$ are of the form

$$\overline{z} = N^{-1}(\overline{z}_0\overline{z}_1) + M \cdot \overline{b},$$

where N, M are two matrices with coefficients in $\mathbb{Q}$, $\overline{b}$ is a finite subset of B, $\overline{z}_0$ is contained in $\mathrm{span}_{\mathbb{Q}}(\overline{b}\overline{c}\overline{d})$ and $\overline{z}_1$ is a generic solution of a perfectly rotund variety defined over $\overline{b}\overline{c}\overline{d}$. Clearly, the possible $N, M, \overline{b}, \overline{z}_0$ and varieties over $\overline{b}\overline{c}\overline{d}$ range in a countable set, and by (CCP) of $K'_E(= K_E)$, also $\overline{z}_1$ ranges in a countable set.

Hence, there are at most countably many generic solutions of $X(\overline{c})$ in $K'_{E'}$, i.e., (CCP) holds on $K'_{E'}$. □

In order to deal with the LIMIT operation, more work is needed.

7. Solutions and roots

We have seen that (CCP) is easy to control at finite operations. However, the LIMIT operation is more difficult to control. In order to do that, we need to carefully count how many solutions of perfectly rotund varieties appear during the construction.

Here we concentrate on how generic solutions can be transferred from one variety to another by multiplication by matrices and translations. The facts proved here will be particularly useful in counting how many times the operation SOLUTIONS can produce new generic solutions of a fixed perfectly rotund variety.

First of all, we wish to point out an easy but fundamental property of $\mathcal{R}(V)$.

Proposition 7.1. *If V is defined over $\overline{c}$, then all the varieties $W \in \mathcal{R}(V)$ are defined over $\operatorname{acl}(\overline{c})$. Moreover, if $W \in \mathcal{R}(V)$, then $\mathcal{R}(W) = \mathcal{R}(V)$. In particular $\mathcal{R}(V) = \mathcal{R}(p \cdot V)$ for any $p \in \mathbb{Z}^\times$.*

Proof. Clearly, if $q \cdot W = p \cdot V$, then W is defined over $\operatorname{acl}(\overline{c})$.

If $W \in \mathcal{R}(V)$, then there are $p, q \in \mathbb{Z}^\times$ such that $q \cdot W = p \cdot V$. If $W' \in \mathcal{R}(V)$ is another variety, there are p', q' such that $q' \cdot W' = p' \cdot V$. Multiplying both sides by p we obtain $pq' \cdot W' = p'q \cdot W$, hence $W' \in \mathcal{R}(W)$. This proves that $\mathcal{R}(V) \subset \mathcal{R}(W)$. The other inclusion follows by exchanging the roles of V and W. □

This means that the families of roots behave like equivalence classes. A similar concept explained with the language of equivalence relations is indeed present in [3], where translations are also considered when defining the equivalence.

From now on, let K_E be a partial E-field.

Definition 7.2. A family $\mathcal{R}(V)$, with $\overline{c}$ defining V, is *completely solved* in K_E if for all $W \in \mathcal{R}(V)$ there is an infinite set of solutions of W algebraically independent over $\operatorname{acl}(\overline{c})$.

By Proposition 5.3, this definition does not depend on the choice of $\overline{c}$.

It is easy to see that (SEC) is equivalent to saying that all the systems $\mathcal{R}(V)$ are completely solved. Indeed, the operation SOLUTIONS applied to V makes sure that $\mathcal{R}(V)$ is completely solved.

The following facts describe the relationships that can occur between the solutions of system of roots for different varieties.

Proposition 7.3. *Let $V \in \mathbb{G}^n$ be an absolutely irreducible rotund variety, and let $M \in \mathcal{M}_{k,n}(\mathbb{Z})$ be an integer matrix.*

If $W \in \mathcal{R}(V)$, then $M \cdot W \in \mathcal{R}(M \cdot V)$.

Proof. If $W \in \mathcal{R}(V)$, then there are $p, q \in \mathbb{Z}^\times$ such that $q \cdot W = p \cdot V$. Multiplying by M we obtain $M \cdot q \cdot W = M \cdot p \cdot V$. However M commutes with $p \cdot \mathrm{Id}$ and $q \cdot \mathrm{Id}$, hence $q \cdot (M \cdot W) = p \cdot (M \cdot V)$, i.e., $M \cdot W \in \mathcal{R}(M \cdot V)$. □

Corollary 7.4. *Let $V \in \mathbb{G}^n$ be an absolutely irreducible rotund variety, and let $M \in \mathcal{M}_{n,n}(\mathbb{Z})$ be a square integer matrix of maximum rank.*

If $W \in \mathcal{R}(M \cdot V)$, then there is a $W' \in \mathcal{R}(V)$ such that $M \cdot W' = W$.

Proof. Let $\tilde{M}$ be the square integer matrix such that $\tilde{M} \cdot M = |\det M| \cdot \mathrm{Id}$. Let $W'' \in \mathcal{R}(M \cdot V)$ be a variety such that $|\det M| \cdot W'' = W$. Let $W' := \tilde{M} \cdot W''$.

Clearly, $M \cdot W' = M \cdot \tilde{M} \cdot W'' = |\det M| \cdot W'' = W$, so the second part of the thesis is satisfied.

Moreover, by definition of $\mathcal{R}(M \cdot V)$ there are $p, q \in \mathbb{Z}^\times$ such that $q \cdot W = p \cdot M \cdot V$. Applying $\tilde{M}$ on both sides, we obtain $q \cdot \tilde{M} \cdot W = p \cdot |\det M| \cdot V$. Replacing W with $M \cdot W'$ we obtain $q \cdot |\det M| \cdot W' = p \cdot |\det M| \cdot V$, hence $W' \in \mathcal{R}(V)$. □

Proposition 7.5. *Let $V \subset \mathbb{G}^n$ be an absolutely irreducible rotund variety, and let $\overline{z} \in \operatorname{dom}(E)^n$.*

If $W \in \mathcal{R}(V \oplus \langle \overline{z}; E(\overline{z}) \rangle)$, then there is a rational number $\frac{p}{q} \in \mathbb{Q}^\times$ and a variety $W' \in \mathcal{R}(V)$ such that $W' \oplus \langle \frac{p}{q}\overline{z}; E(\frac{p}{q}\overline{z}) \rangle = W$.

Proof. By definition, there are $p, q \in \mathbb{N}^\times$ such that $q \cdot W = p \cdot (V \oplus \langle \overline{z}; E(\overline{z})\rangle)$. Let $W' := W \oplus \langle -\frac{p}{q}\overline{z}; E(-\frac{p}{q}\overline{z})\rangle$. The second part of the thesis is satisfied.

Moreover,

$$q \cdot W' = q \cdot \left(W \oplus \langle -\frac{p}{q}\overline{z}; E(-\frac{p}{q}\overline{z})\rangle \right) = q \cdot W \oplus \langle -p \cdot \overline{z}; E(-p \cdot \overline{z})\rangle = p \cdot V.$$

Hence, $W' \in \mathcal{R}(V)$. □

Using the above propositions we can finally see something about how generic solutions of one system of roots move to solutions of another system. The following result is not useful yet in the proof of the main theorem, but it is the kind of statement we are looking for. It is also useful for other constructions, as shown in Section 12.

Proposition 7.6. *Let $V \subset \mathbb{G}^n$ be an absolutely irreducible rotund variety. Let $M \in \mathcal{M}_{n,n}(\mathbb{Z})$ be a square integer matrix of maximum rank and $\overline{z} \in \operatorname{dom}(E)^n$.*

The family $\mathcal{R}(V)$ is completely solved if and only if $\mathcal{R}(M \cdot V \oplus \langle \overline{z}; E(\overline{z})\rangle)$ is.

Proof. It is sufficient to verify the left-to-right direction of the implication. Indeed, if $\tilde{M}$ is the integer matrix such that $\tilde{M} \cdot M = |\det M| \cdot \mathrm{Id}$, we can also write $|\det M| \cdot V = \tilde{M} \cdot X \oplus \langle -\tilde{M} \cdot \overline{z}; E(-\tilde{M} \cdot \overline{z})\rangle$. Since $\mathcal{R}(|\det M| \cdot V) = \mathcal{R}(V)$, the roles of X and V can be exchanged to reverse the argument. Hence, from now on let us suppose that $\mathcal{R}(V)$ is completely solved.

Let $W \in \mathcal{R}(M \cdot V \oplus \langle \overline{z}; E(\overline{z})\rangle)$. By the above propositions, there is a $W' \in \mathcal{R}(V)$ and a rational number $\frac{p}{q} \in \mathbb{Q}^\times$ such that $M \cdot W' \oplus \langle \frac{p}{q}\overline{z}; E(\frac{p}{q}\overline{z})\rangle = W$.

Let $\overline{c}$ be a finite set of parameters defining W' containing also $\overline{z}, E(\overline{z})$. Clearly, W is defined also over $\overline{c}$, and if $\overline{x}$ is a generic solution of $W'(\overline{c})$, then $M \cdot \overline{x} + \frac{p}{q}\overline{z}$ is a generic solution of $W(\overline{c})$.

Moreover, we claim that the map $P \mapsto M \cdot P \oplus \langle \frac{p}{q}\overline{z}; E(\frac{p}{q}\overline{z})\rangle$, for $P \in W'$, preserves the algebraic independence over $\overline{c}$. As the translation by $\langle \frac{p}{q}\overline{z}; E(\frac{p}{q}\overline{z})\rangle$ is an algebraic invertible map defined over $\operatorname{acl}(\overline{c})$, it is sufficient to check this on the map $P \mapsto M \cdot P$.

However, since M is invertible, there is an integer matrix $\tilde{M}$ such that $\tilde{M} \cdot M = |\det M| \cdot \mathrm{Id}$; in particular, the composition $P \mapsto M \cdot P \mapsto \tilde{M} \cdot M \cdot P = |\det M| \cdot P$ is just the map $P \mapsto |\det M| \cdot P$. This map is algebraic and finite-to-one, hence it preserves the algebraic independence; in particular, $P \mapsto M \cdot P$ must preserve the algebraic independence.

This implies that an infinite set of algebraically independent solutions of W' is mapped to an infinite set of algebraically independent solutions of W. In particular, if $\mathcal{R}(V)$ is completely solved, then W contains an infinite set of algebraically independent solutions over $\overline{c}$. Since this holds for any W, $\mathcal{R}(M \cdot V \oplus \langle \overline{z}; E(\overline{z})\rangle)$ is completely solved. □

Something stronger is needed for our construction, as we do not just add generic solutions to simple varieties, but we force them to be dense, and moreover the solutions satisfy a transcendence condition which is more than being generic. The necessary machinery to deal with these problems will be detailed in the next sections.

8. $\mathbb{G}$-restriction of the scalars

During our construction, we add solutions to simple varieties that are not just generic, but something more. We put this into a definition.

Definition 8.1. If V is an absolutely free rotund variety $V(\overline{c}) \subset \mathbb{G}^n$, with $\overline{c}$ closed under σ, a generic solution $\overline{z} \in K^n$ is *real generic* if

$$\operatorname{tr.deg.}_{\overline{c}}\langle \Re(\overline{z})\Im(\overline{z}); E(\Re(\overline{z})\Im(\overline{z}))\rangle = 2\dim V.$$

A set of real generic solutions $\mathcal{S}$ of $V(\overline{c})$ is *really algebraically independent* if for any finite subset $\{\overline{z}_1, \dots, \overline{z}_k\} \subset \mathcal{S}$ the following holds:

$$\begin{aligned}\operatorname{tr.deg.}_{\overline{c}}(\langle \Re(\overline{z}_1)\Im(\overline{z}_1); E(\Re(\overline{z}_1)\Im(\overline{z}_1))\rangle, \dots, \langle \Re(\overline{z}_k)\Im(\overline{z}_k); E(\Re(\overline{z}_k)\Im(\overline{z}_k))\rangle) = \\ = 2k \cdot \dim V.\end{aligned}$$

In the operation SOLUTIONS we are adding real generic solutions to simple varieties. Thus, we are actually adding generic solutions to some varieties whose dimension is double. We give them a name and a precise description.

Definition 8.2. We define the group $\mathbb{G}_R := (R \times R_{>0}) \times (iR \times \mathbb{S}^1(K)) \subset \mathbb{G}^2(K)$ and the *realization* map $r : \mathbb{G} \to \mathbb{G}_R$ as follows:

$$r \,:\, (z, w) \mapsto (\Re(z), |w|) \times (i\Im(z), \Theta(w)).$$

We extend r as a map $\mathbb{G}^n \to \mathbb{G}^{2n}$ in the following way

$$r : \langle \overline{z}; \overline{w}\rangle \mapsto \langle \Re(\overline{z}); |\overline{w}|\rangle \times \langle \Im(\overline{z}); \Theta(\overline{w})\rangle.$$

It would have been more natural to define r as the natural coordinate-wise application $\mathbb{G}^n \to \mathbb{G}_R^n$; however, we will need to manipulate matrices, and the above extension of r to $\mathbb{G}^n$ is much better suited for the task.

We apply the map r to the points of rotund varieties.

Definition 8.3. Let V be a subvariety of $\mathbb{G}^n$ for some n.

(1) the *realization* of V is the set $r(V) := \{r(\langle \overline{z}; \overline{w}\rangle) \in \mathbb{G}^{2n} \,:\, \langle \overline{z}; \overline{w}\rangle \in V\}$;
(2) the $\mathbb{G}$-*restriction of the scalars* of V is the Zariski closure of $r(V)$ in $\mathbb{G}^{2n}$; it will be denoted by $\check{V}$.

In the operation SOLUTIONS, when we take a variety $W \in \mathcal{R}(V)$, we add generic solutions to $\check{W}$; moreover, we choose the new solutions inside $r(W)$, and we make sure that they are dense in $r(W)$.

Remark 8.4. The group $\mathbb{G}_R$ can be thought as a semi-algebraic group over R replacing iR with R and $\mathbb{S}^1(K)$ with $\{(x, y) \in R^2 \,:\, x^2 + y^2 = 1\}$. Then $r(V)$ can be seen as a semi-algebraic subvariety of $\mathbb{G}_R^n$.

The algebraic variety $\check{V}$ is similar to the classical Weil restriction of the scalars. However, unlike the classical case, while the points of $r(V)$ are in bijection with the points of V, the set of the 'real points' of $\check{V}$ is *larger* than $r(V)$.

The study of the $\mathbb{G}$-restriction of rotund varieties is quite crucial for proving that our construction yields a Zilber field. It is essential to prove that both (SP) and (CCP) holds in the final structure.

9. Rotundity for $\mathbb{G}$-restrictions

In order to prove that (SP) and (CCP) holds in the structure resulting from Section 3, we first state a structure theorem for the $\mathbb{G}$-restriction $\check{V}$ of a rotund variety V. Our first problem is to determine whether the $\mathbb{G}$-restriction of an absolutely free, rotund variety is itself absolutely free and rotund.

Moreover, if V is simple, one could ask if $\check{V}$ is also simple, but this is always false, as the following trivial equation implies:

$$\dim\begin{pmatrix} \mathrm{Id} & \mathrm{Id}\end{pmatrix} \cdot \check{V} = \dim V = \operatorname{rank}\begin{pmatrix} \mathrm{Id} & \mathrm{Id}\end{pmatrix}.$$

We prove here that $\check{V}$ is indeed absolutely free and rotund, and that the above example describes essentially the only way in which $\check{V}$ is not simple.

Theorem 9.1. *Let V be an absolutely irreducible simple variety. Then $\check{V}$ is an absolutely free, absolutely irreducible rotund variety.*

Moreover, if $\dim M \cdot \check{V} = \mathrm{rank} M$ *for some non-zero integer matrix of maximum rank, then V is perfectly rotund, and one of the following holds:*

(1) $\mathrm{rank} M = 2n$*;*
(2) $\mathrm{rank} M = n$*, and M is of the form*

$$M = \begin{pmatrix} N & Q \end{pmatrix}$$

where N, Q are two square invertible matrices.

The proof requires several steps. From now on, let us suppose that $\check{V}$ is defined over some $\overline{c}$.

Proposition 9.2. *If $V \subset \mathbb{G}^n$ is absolutely free, then $\check{V}$ is absolutely free.*

Proof. Let $x_1, \dots, x_n, y_1, \dots, y_n$ be the additive coordinates of $\check{V}$; by x_i we mean the coordinates coming from the real parts of V, and by y_i the imaginary parts.

Let us suppose that for some constant c and some integers $m_1, \dots, m_n, p_1, \dots, p_n$ the following

$$m_1 x_1 + \cdots + m_n x_n + p_1 y_1 + \cdots + p_n y_n = c$$

is constantly true on all $\check{V}$. In particular, it is true on the points of $r(V)$; this implies that

$$\begin{aligned} m_1 x_1 + \cdots + m_n x_n &= \Re(c), \\ p_1 y_1 + \cdots + p_n y_n &= i\Im(c) \end{aligned}$$

constantly on $\check{V}$. This means that

$$\begin{aligned} \Re(m_1 z_1 + \cdots + m_n z_n) &= \Re(c), \\ \Im(p_1 z_1 + \cdots + p_n z_n) &= i\Im(c) \end{aligned}$$

constantly on V. By strong minimality, this implies that $m_1 z_1 + \cdots + m_n z_n$ and $p_1 z_1 + \cdots + p_n z_n$ have both finite image, but by absolute freeness of V, this implies $m_1 = \cdots = m_n = 0$ and $p_1 = \cdots = p_n = 0$.

The same argument applied to the multiplicative coordinates $\rho_1, \dots, \rho_n, \theta_1, \dots, \theta_n$ yields the absolute freeness of V. $\square$

Proposition 9.3. *If $V \subset \mathbb{G}^n$ is absolutely irreducible, then $\check{V}$ is absolutely irreducible.*

Proof. Let V' be an absolutely irreducible variety such that $2 \cdot V' = V$.

There is a map $V' \times (V')^\sigma \mapsto \mathbb{G}^{2n}$ described by the following equation:

$$\prod_{i=1}^{n}(z_i, w_i) \times \prod_{i=1}^{n}(z'_i, w'_i) \mapsto \prod_{i=1}^{n}(z_i + z'_i, w_i w'_i) \times \prod_{i=1}^{n}\left(z_i - z'_i, \frac{w_i}{w'_i}\right).$$

It is clear that on the Zariski dense subset of $V' \times (V')^\sigma$ described by the points $P \times P^\sigma$, for $P \in V'$, the image is exactly $r(V)$; taking the Zariski closure, we obtain that this is a surjective map from $V' \times (V')^\sigma$ to $\check{V}$.

However, $V' \times (V')^\sigma$ is an absolutely irreducible variety, as it is a product of two absolutely irreducible varieties; hence $\check{V}$ is also absolutely irreducible. $\square$

In particular, when V is an absolutely irreducible simple variety, as it is in our construction, the variety $\check{V}$ is absolutely free and absolutely irreducible. We still have to verify if it is rotund, and how far it is from being simple.

From now on, let us suppose that M is a non-zero integer matrix in $\mathcal{M}_{k,2n}(\mathbb{Z})$ of maximum rank, and that V is an absolutely irreducible simple variety. We want to determine as much as possible on $\dim M \cdot \check{V}$.

First of all, we need to reduce a bit the complexity of the matrix M.

Proposition 9.4. *There is a matrix $A \in \mathcal{M}_{k,k}(\mathbb{Z})$ of maximum rank such that $A \cdot M$ is of the following form*

$$A \cdot M = \left(\begin{array}{cc} & 0 \\ M_1 & P_1 \\ & Q_1 \\ \hline 0 & P_2 \\ 0 & Q_2 \end{array} \right)$$

with the following properties:

(1) M_1 has n columns;
(2) the rows of M_1 are $\mathbb{Q}$-linearly independent;
(3) the rows of M_1, P_1 and P_2 are $\mathbb{Q}$-linearly independent;
(4) the rows of P_1, P_2, Q_1 and Q_2 are $\mathbb{Q}$-linearly independent.

Proof. It amounts to using row operations in the correct order on M.

First of all, we look at the first n columns of the matrix, and we use the row operations to eliminate all the redundant vectors until we are left with some $\mathbb{Q}$-linearly independent rows, which we reorder to be in the first part of the matrix. In this way, we split the matrix into an upper half and a lower half, where the lower half has zero entries in the first n columns, and the upper half restricted to the same columns has rank equal to the number of its rows.

Now, we concentrate on the other n columns. The lower half of the matrix is made of $\mathbb{Q}$-linearly independent rows, by the original hypothesis on the rank of M. We leave them untouched, while using them in the upper half in order to eliminate the redundancies again. The row operations on the upper half cannot harm the $\mathbb{Q}$-linear independence of the first n columns. We reorder the rows so to have all the zeroes of the last n columns at the beginning, as in the figure.

At the end of these operations, we have defined M_1 as the north-west corner; we just have to look at a maximal set of rows for the last n columns which is $\mathbb{Q}$-linearly independent over the rows of M_1 in order to define who P_1, P_2, Q_1 and Q_2 are. □

Note that $\dim(A \cdot M \cdot \check{V}) = \dim(M \cdot \check{V})$, as A is invertible over $\mathbb{Q}$. Let us suppose that M is already of the above form.

Let $\check{M}$ be the matrix

$$\check{M} := \begin{pmatrix} M_1 \\ P_1 \\ P_2 \end{pmatrix}.$$

By construction, $\check{M}$ has rank equal to the number of its rows. It is clear that all the coordinate functions of $M \cdot \check{V}$, when restricted to $M \cdot r(V)$, are actually sums and products of the coordinate functions of $r(\check{M} \cdot V)$.

In the following, we will take an algebraically independent subset S of the coordinate functions of $M \cdot \check{V}$. Taking the restrictions to the subset $M \cdot r(V) \subset M \cdot \check{V}$, we will try to estimate the actual size of $M \cdot \check{V}$ by studying how large is the image of $M \cdot r(V)$ through the functions in S.

Each function in such an S is of the form $\overline{m} \cdot \overline{x} + \overline{q} \cdot \overline{y}$ or $\overline{\rho}^{\overline{m}} \overline{\theta}^{\overline{q}}$, where $(\overline{m}, \overline{q})$ is a row of M. We introduce the following notation.

Notation 9.5. If S is a set of coordinates as above, we denote by $r(S)$ the set containing $\overline{m} \cdot \overline{x}$, $\overline{q} \cdot \overline{y}$, $\overline{\rho}^{\overline{m}}$, $\overline{\theta}^{\overline{q}}$ for each $\overline{m} \cdot \overline{x} + \overline{q} \cdot \overline{y}$ or $\overline{\rho}^{\overline{m}} \overline{\theta}^{\overline{q}}$ in S.

We know that in general $\text{tr.deg.}_{\overline{c}}(S) \geq \text{tr.deg.}_{\overline{c}}(r(S))/2$, but this is far from being enough for our purposes. Hence, we need to distinguish, among the coordinate functions in S, the ones that vary in a one-dimensional set, and the ones that vary in a two-dimensional set.

The situation can be ambiguous: the set $\{x_1 + iy_1, x_2 + iy_1\}$ is algebraically independent, provided that z_1 and z_2 are, and the image of both functions applied to $r(V)$ is two-dimensional; but when we choose the value of one function, the other is confined in a one-dimensional subset of its codomain.

This means that the order in which we consider the functions matters; we want to say that when we take $x_1 + iy_1$ first, it is two-dimensional, and then that $x_2 + iy_2$ is one-dimensional. Thus, we study sequences of algebraically independent coordinate functions of $M \cdot \check{V}$ rather than just sets.

Using sequences, we can define the dimension of a coordinate function in an unambiguous way. Let $(s_j)_{j<|S|}$ be a particular enumeration of S.

Definition 9.6. A coordinate function $s_k \in S$ is *one-dimensional* (resp. *two-dimensional*) if $\text{tr.deg.}_{\overline{c},r(s_0,\ldots,s_{k-1})} r(s_k)$ is one (resp. two).

The following remark is rather trivial.

Proposition 9.7. *Let S be a set of algebraically independent coordinate functions of $M \cdot \check{V}$ enumerated as $(s_j)_{j<|S|}$. If S contains k_1 one-dimensional functions, and k_2 two-dimensional functions, then $|S| = k_1 + k_2$ and* $\text{tr.deg.}_{\overline{c}}(r(S)) = k_1 + 2k_2$.

This is our desired correction: $\text{tr.deg.}_{\overline{c}} S > \text{tr.deg.}_{\overline{c}}(r(S))/2$ as soon as there are one-dimensional functions. Moreover, their number is independent from the ordering of S.

We want now to find a set S of algebraically independent functions containing many one-dimensional functions. Clearly, for such a set S we have $\dim(M \cdot \check{V}) \geq |S|$. In order to do that, we start from a classical combinatorial lemma [2] applied to the matroid given by the algebraic closure. We just state the special instance needed for our proof.

Lemma 9.8 (Hall's Marriage Lemma)**.** *Let $X = \{x_j\}_{1\leq j\leq n}$ and $Y = \{y_j\}_{1\leq j\leq n}$ be two subsets of some field L, and $\overline{c}$ some finite subset of L.*

If $\text{tr.deg.}_{\overline{c}} \bigcup_{j\in T}\{x_j, y_j\} \geq |T|$ for all $T \subset \{1, \ldots, n\}$, then there is a subset $Z \subset X \cup Y$ such that

(1) $|Z \cap \{x_j, y_j\}| = 1$ for all $j \in \{1, \ldots, n\}$;
(2) $\text{tr.deg.}_{\overline{c}} Z = |Z| = n$.

If we take $L = K(W)$, where $W \subset \mathbb{G}^n$ is some rotund variety defined over some $\overline{c} \subset K$, and we take as X the additive coordinate functions of V and as Y the multiplicative coordinate functions of V, then by rotundity the hypothesis of Lemma 9.8 are satisfied. Hence, we can choose an algebraically independent set of coordinate functions such that for each factor $\mathbb{G}$ of $\mathbb{G}^n$ exactly one of the two functions appear in the set.

Proposition 9.9. *There is an algebraically independent set of coordinate functions S_0 for $M \cdot \check{V}$ such that $|S_0| \geq \text{rank} M$.*

In particular, $\dim M \cdot \check{V} \geq \text{rank} M$, and $\check{V}$ is rotund.

Proof. Let us apply Lemma 9.8 to the coordinate functions of $\check{M} \cdot V$: we find that there is an algebraically independent set of functions such that for each row $\overline{m}$ of $\check{M}$, exactly one of $\overline{m} \cdot \overline{z}$ or $\overline{w}^{\overline{m}}$ is in it.

If we split them into real and imaginary parts, writing $\overline{z} = \overline{x} + \overline{y}$ and $\overline{w} = \overline{\rho}\overline{\theta}$, then they are some of the coordinate functions of $r(\check{M} \cdot V)$. Let C_0 be the set of the coordinate functions of $r(\check{M} \cdot V)$, and let H_0 be the subset of C_0 found above using Hall's Marriage Lemma. By construction, $\text{tr.deg.}_{\overline{c}}(C_0) = 2 \dim \check{M} \cdot V$, while H_0 is algebraically independent and $|H_0| = 2\text{rank} M$.

First of all, note that if we exchange one row of M_1 with one suitable row of Q_1, Q_2, the linear span of the rows of M_1, P_2, P_2 does not change. Moreover, we can iterate this procedure until we have used all the rows of Q_1, Q_2.

After this procedure, if the row $\overline{m}$ has been replaced by $\overline{q}$, we replace the functions $\overline{m} \cdot \overline{y}$, $\overline{\theta}^{\overline{m}}$ with respectively $\overline{q} \cdot \overline{y}$, $\overline{\theta}^{\overline{q}}$. Let C_1 and H_1 the two sets of functions obtained by C_0 and H_0 using the above substitutions. Obviously, we have $\mathrm{acl}(C_0\overline{c}) = \mathrm{acl}(C_1\overline{c})$ and $\mathrm{acl}(H_0\overline{c}) = \mathrm{acl}(H_1\overline{c})$. In particular, we also have that H_1 is still algebraically independent over $\overline{c}$.

At last, let C_2 and H_2 be the functions in C_1 and H_1 resp. that actually appear in $r(M \cdot \check{V})$; i.e., the functions $\overline{m} \cdot \overline{x}$, $\overline{q} \cdot \overline{y}$, $\overline{\rho}^{\overline{m}}$, $\overline{\theta}^{\overline{q}}$ such that $\overline{m}$ is a row of M_1 and $\overline{q}$ is a row of one of P_1, P_2, Q_1, Q_2. Note that C_2 is $r(B)$, with B the set of all the coordinate functions of $M \cdot r(V)$.

Let us call m the number of rows of M of the form $(\overline{m}, \overline{q})$ with both $\overline{m}, \overline{q}$ not zero. By construction, $\mathrm{tr.deg.}_{\overline{c}}(H_2) = \mathrm{rank}M + m$ and $\mathrm{tr.deg.}_{\overline{c}}(C_2) \geq \mathrm{rank}M + m$.

Hence, combining the functions in C_2 we obtain all the coordinate functions of $M \cdot r(V)$. First of all, we take all the rows $(\overline{m}, \overline{q})$ of M such that either $\overline{m}$ or $\overline{q}$ are zero. If $\overline{m} \neq 0$, then exactly one of $\overline{m} \cdot \overline{x}$ and $\overline{\rho}^{\overline{m}}$ is in H_2; similarly, if $\overline{q} \neq 0$, exactly one of $\overline{q} \cdot \overline{y}$ and $\overline{\theta}^{\overline{q}}$ is in H_2. Let us call S the set of all such elements in H_2. Clearly, S is algebraically independent, and moreover, each function $x \in S$ is automatically one-dimensional.

Now, let us take a maximal algebraically independent set S_0 of coordinate functions of $M \cdot r(V)$ containing S. We claim that S_0 is our desired set.

Indeed, let us take an enumeration $(s_j)_{j<|S|}$ of S_0 starting with the elements of S. Let us call k_1 the number of one-dimensional coordinates of that enumeration, and k_2 the two-dimensional ones. By construction, $k_1 \geq \mathrm{rank}M - m$.

Clearly, $\mathrm{tr.deg.}_{\overline{c}}(r(S_0)) = \mathrm{tr.deg.}_{\overline{c}}(C_2) \geq \mathrm{rank}M + m$. Since $\mathrm{tr.deg.}_{\overline{c}}(r(S_0)) = k_1 + 2k_2$, this implies

$$k_1 + 2k_2 \geq \mathrm{rank}M + m.$$

Together with $k_1 \geq \mathrm{rank}M - m$ we obtain

$$2|S_0| = 2(k_1 + k_2) \geq 2\mathrm{rank}M$$

as desired. □

Giving a better look at the proof, however, we can say more. From now on, let S_0 be the set of algebraically independent functions found above.

Let us introduce another definition.

Definition 9.10. A coordinate function x in S of $M \cdot \check{V}$ is *pure* if its dimension is the same in any ordering of S.

The set S is said to be *pure* if all of its functions are pure.

Proposition 9.11. *If* $\dim M \cdot \check{V} = \mathrm{rank}M$*:*

(1) S_0 *is pure;*
(2) V *is perfectly rotund;*
(3) $\mathrm{rank}\check{M} = n$.

Proof. The restriction $\dim M \cdot \check{V} = \mathrm{rank}M$ implies $|S_0| = \mathrm{rank}M$, and this forces two equalities: $k_2 = m$, $k_1 = \mathrm{rank}M - m$.

The first equality $k_1 = \mathrm{rank}M - m$ implies that all the one-dimensional coordinates are exactly the first $(\mathrm{rank}M - m)$ ones we added to S_0. They correspond to the rows of M of the form $(\overline{m}, 0)$ or $(0, \overline{q})$, so they are pure by construction.

Since $\mathrm{tr.deg.}_{\overline{c}}(r(M \cdot r(V))) = k_1 + 2k_2$, and k_1 functions are already pure and one-dimensional, the remaining k_2 functions are forced to be all two-dimensional in whatever order we take them. Hence, S_0 is pure.

Moreover, the equality in the above proposition implies that $\text{tr.deg.}_{\overline{c}}(C_2) = |H_2|$. By construction, this implies that for each row of $\check{M}$ we can take *exactly* one function in Hall's Marriage Lemma, and no more, as the rest becomes algebraic; in particular, we must have $\dim \check{M} \cdot V = \text{rank}\check{M}$.

Since V is simple, this implies $\text{rank}\check{M} = n$, and that V is perfectly rotund. □

We can still refine the statement. First, we analyze the special subcase when S_0 is composed only of one-dimensional functions. In order to fully comprehend this case, we first need to establish the following two algebraic facts, which both derive from the following classical statement.

Lemma 9.12 (Puiseux series)**.** *Let z, w be two non-constant functions on an algebraic curve $\mathcal{C}$ defined over $\mathbb{C}$. Then for some number $a \in \mathbb{C}$ and integers k, d the following holds:*

$$w = az^{\frac{k}{d}} + O(z^{\frac{k+1}{d}}).$$

Moreover, k and d can be bounded uniformly in terms of the degree of $\mathcal{C}$.

Thanks to the bounds on k and d, this can be seen as a first order statement over $\mathbb{R}$; hence, it is true over every real closed field. We use it to prove the algebraic independence of the various realizations of the coordinate functions.

Lemma 9.13. *Let V be an absolutely irreducible algebraic variety such that $\check{V}$ is defined over some $\overline{c}$. Let B be some set of algebraically independent functions on V, and let w be a function on V contained in $\text{acl}(B\overline{c})$.*

If $|w| \in \text{acl}(\{|z| : z \in B\} \cup \overline{c})$, or if $\Theta(w) \in \text{acl}(\{\Theta(z) : z \in B\} \cup \overline{c}\})$, then there is a non-trivial monomial constant relation between the functions in B and w.

Proof. We may assume that B is minimal, i.e., that $w \notin \text{acl}(B \cup \{\overline{c}\} \setminus \{z\})$ for all $z \in B$. If $B = \emptyset$, then $w \in \text{acl}(\overline{c})$, and we are done. We proceed by induction on $|B|$. Let us suppose $|B| \geq 1$.

Let us take one function $z \in B$. By minimality of B, there is a polynomial relation

$$p(z, w) = 0$$

with coefficients in $\mathbb{Q}(\overline{c}, B \setminus \{z\})$. Let us specialize all the variables in $B \setminus \{z\}$ such in a way that the above polynomial contains occurrences of both z and w.

By Lemma 9.12 applied twice, the following is true on some open subset of the specialization of V:

$$w = az^{\frac{k}{d}} + bz^{\frac{k+m}{d}} + O(z^{\frac{k+m+1}{d}}),$$

for some integer k, some natural numbers $m, d > 0$ and for some $a, b \in \text{acl}(\overline{c}, B\setminus\{z\})$. We are taking the first two terms of the Puiseux series: hence, if $a = 0$ or $k = 0$, then $w = 0$, and if $b = 0$, then $az^{\frac{k}{d}} = w$. Since $|B| \geq 1$, w cannot be constant, so we may assume $a \neq 0$ and $k \neq 0$.

Let us study the case of $|w|$. Taking the modulus,

$$|w| = \left|az^{\frac{k}{d}} + bz^{\frac{k+m}{d}}\right| + O\left(\left|z^{\frac{k+m+1}{d}}\right|\right).$$

Let us suppose that $b \neq 0$. It is clear that as $|z|$ gets smaller, then the value $|w|$ must take more and more different values as $\Theta(z)$ varies. But $\Theta(z)$ is algebraically independent from $\text{acl}(\{|x| : x \in B\} \cup \overline{c})$, so even when we fix the values of the $|x|$ for $x \in B$, it is still free to vary in $\mathbb{S}^1(K)$ except for a finite set of uniformly bounded cardinality; hence $|w|$ is algebraically independent too. This contradicts our hypothesis, so $b = 0$.

If instead we take $\Theta(w)$, then

$$\Theta(w) = \Theta\left(az^{\frac{k}{d}} + bz^{\frac{k+m}{d}}\right) + O\left(\left|z^{\frac{k+m+1}{d}}\right|\right).$$

As above, if $b \neq 0$, then it is clear that if we fix some $\Theta(z)$ out of a finite set, when $|z|$ gets smaller, $\Theta(w)$ must take more and more different values. Again, $|z|$ is free to vary in $R_{>0}$ except for a finite set of bounded cardinality. This implies that $\Theta(w)$ is algebraically independent from $\operatorname{acl}(\{|x| : x \in B\} \cup \overline{c})$, against the hypothesis. Thus $b = 0$.

However, when $b = 0$ there is no rest term, hence we actually have the equality $w = az^{\frac{k}{d}}$, i.e., $w^d = a^d z^k$. This means that the function $w^d z^{-k}$ is in $\operatorname{acl}(B \cup \overline{c} \setminus \{z\})$. In turn, $|w^d z^{-k}|$ must also be in $\operatorname{acl}(\{|x| : x \in B \setminus \{z\}\} \cup \overline{c})$, or $\Theta(w^d z^{-k})$ must be in $\operatorname{acl}(\{\Theta(x) : x \in B \setminus \{z\}\} \cup \overline{c})$. By inductive hypothesis, there is a monomial constant relation between $w^d z^{-k}$ and the functions in $B \setminus \{z\}$. Clearly, this induces a monomial constant relation between w and the functions in B, as desired. □

Lemma 9.14. *Let V be an absolutely irreducible algebraic variety such that V is defined over some $\overline{c}$. Let B be some set of algebraically independent functions on V, and let w be a function on V contained in* $\operatorname{acl}(B\overline{c})$.

The function $|w|$ (or $\Theta(w)$) cannot be interalgebraic with $\Re(z)$, $\Im(z)$, or $\Theta(z)$ (resp. $|z|$) over $r(B \setminus \{z\}) \cup \overline{c}$ for any $z \in B$.

Proof. Let us suppose by contradiction that the thesis is false. This implies that w is interalgebraic with z over $B \setminus \{z\} \cup \overline{c}$. As above, we find a polynomial such that

$$p(z, w) = 0$$

and a piece of Puiseux series. This time, we take just one term.

For $|w|$, we calculate the modulus:

$$|w| = \left|az^{\frac{k}{d}}\right| + O\left(\left|z^{\frac{k+1}{d}}\right|\right).$$

However, as $\Re(z)$ gets smaller, then $|w|$ still varies in larger and larger sets by moving $\Im(z)$, and vice versa. Similarly, if we fix some value $\Theta(z)$ then $|w|$ still varies by moving $|z|$ sufficiently near to 0.

For $\Theta(w)$:

$$\Theta(w) = \Theta\left(az^{\frac{k}{d}}\right) + O\left(\left|z^{\frac{k+1}{d}}\right|\right).$$

If we fix a value $\Re(z)$ small enough, then $\Theta(w)$ still varies by moving $\Im(z)$, and vice versa. Similarly, if we fix a sufficiently small value $|z|$ then $\Theta(w)$ still varies by moving $\Theta(z)$.

Both of the above consequences contradict interalgebraicity, unless $a = 0$; but this implies that w is constant with respect to z, a contradiction again. □

Proposition 9.15. *If* $\dim M \cdot \check{V} = \operatorname{rank} M$*, and all the functions in S_0 are one-dimensional, then* $\operatorname{rank} M = 2n$.

Proof. We are in the case $\operatorname{rank}\check{M} = n$ and V perfectly rotund.

In this situation we have that the functions in S_0 come from the rows of M of the form $(\overline{m}, 0)$ or $(0, \overline{q})$; in other words, when $P_1 = Q_1 = 0$. Hence we are just extracting an algebraically independent subset of C_2, without combining any functions.

Case $Q_2 \neq 0$. If $\operatorname{rank} Q_2 = \operatorname{rank} M_1 = n$, we are done; hence, let us assume that $\operatorname{rank} Q_2 < n$.

In this case, let $\check{M}'$ be the submatrix of $\check{M}$ of the rows that gets substituted by the rows of Q_2. Note that $\operatorname{rank}\check{M}' = \operatorname{rank} Q_2$, by definition of Q_2, and $\operatorname{rank}\check{M}' < \operatorname{rank}\check{M} = n$.

Let us take one row $\overline{m}$ of $\check{M}$ which is not in $\check{M}'$. Then exactly one of the two pairs $(\overline{m} \cdot \overline{x}, \overline{m} \cdot \overline{y})$ and $(\overline{\rho}^{\overline{m}}, \overline{\theta}^{\overline{m}})$ is in H_0. Since V is simple, then $\dim \check{M}' \cdot V > \operatorname{rank}\check{M}'$; in particular, we can replace the function $(\overline{m} \cdot \overline{x} + \overline{m} \cdot \overline{y})$ (resp. $\overline{\rho}^{\overline{m}} \overline{\theta}^{\overline{m}}$) with some

other function $(\overline{m}' \cdot \overline{x} + \overline{m}' \cdot \overline{y})$ or $\overline{\rho}^{\overline{m}'} \overline{\theta}^{\overline{m}'}$ not in H_0, with $\overline{m}'$ a row of $\check{M}'$, in order to obtain a corresponding H_0' such that $\operatorname{acl}(H_0\overline{c}) = \operatorname{acl}(H_0'\overline{c})$.

Let us suppose that $\overline{m}'$ gets replaced by $\overline{q}'$. Let us apply the replacement we used to define H_1 to H_0', and let us call H_1' the resulting set. Note that at this point, H_1' contains the functions $\overline{m}' \cdot \overline{x}$ and $\overline{q}' \cdot \overline{y}$, or the functions $\overline{\rho}^{\overline{m}'}$ and $\overline{\theta}^{\overline{q}'}$.

Again, let H_2' be the set of the functions in H_1' that actually appear among the coordinate functions of $r(M \cdot \check{V})$. Note that H_2' is algebraically independent over $\overline{c}$, as H_1' is.

By construction, H_2' contains all the functions in H_2, with exactly one exception: the unique function in H_2 in the set $\{\overline{m} \cdot \overline{x}, \overline{m} \cdot \overline{y}, \overline{\rho}^{\overline{m}}, \overline{\theta}^{\overline{m}}\}$. Moreover, H_2' contains two new functions coming from $H_1' \setminus H_1$, as all the functions $\overline{m}' \cdot \overline{x}$, $\overline{q} \cdot \overline{y}$, $\overline{\rho}^{\overline{m}'}$, $\overline{\theta}^{\overline{q}}$ appear as coordinate functions of $r(M \cdot \check{V})$. This implies that $|H_2'| > |H_2|$.

However, while $|H_2| = \operatorname{rank} M$, $\dim M \cdot \check{V} \geq |H_2'| > |H_2| = \operatorname{rank} M$, and since S_0 contains only one-dimensional functions, it contains H_2, and this contradicts the hypothesis.

Case $Q_2 = 0$. We claim that in this case there is a multiplicative dependency among the multiplicative coordinates of V, against the hypothesis that V is absolutely free.

Since V is absolutely free, we can choose an algebraically independent set B of coordinates of V containing at least one additive coordinate. Moreover, since V is perfectly rotund, at least one multiplicative coordinate must not be in B. Let $\overline{w}^{\overline{q}} = \overline{\rho}^{\overline{q}} \overline{\theta}^{\overline{q}}$ be this function.

By hypothesis, $\overline{w}^{\overline{q}}$ is algebraic over $B \cup \overline{c}$. Since V is absolutely free, $\overline{w}^{\overline{q}}$ is not a constant function; in particular, there must some elements $\psi \in B$ such that $\overline{w}^{\overline{q}}$ is interalgebraic with ψ over $B \setminus \{\psi\} \cup \overline{c}$.

If there is one such ψ of the form $\psi = \overline{m} \cdot \overline{z} = \overline{m} \cdot \overline{x} + \overline{m} \cdot \overline{y}$ for some $\overline{m}$, then, by Lemma 9.14, the functions $\overline{\rho}^{\overline{q}}$ and $\overline{\theta}^{\overline{q}}$, taken separately, are algebraically independent from $r(B \setminus \{\psi\}) \cup \{\overline{m} \cdot \overline{x}\} \cup \overline{c}$ and also from $r(B \setminus \{\psi\}) \cup \{\overline{m} \cdot \overline{y}\} \cup \overline{c}$.

Let us suppose instead that all the possible ψ's are of the form $\psi = \overline{\rho}^{\overline{m}} \overline{\theta}^{\overline{m}}$. If $\overline{\rho}^{\overline{q}}$ is algebraically dependent on $r(B \setminus \{\psi\}) \cup \{\overline{\rho}^{\overline{m}}\} \cup \overline{c}$ for all the possible ψ's, then it is actually contained in $\operatorname{acl}(\{|z| \,:\, z \in B\} \cup \overline{c})$. By Lemma 9.13, there is a monomial constant relation between the functions in B, against the hypothesis of absolute freeness of V; hence, one of the possible ψ's is such that $\overline{\rho}^{\overline{q}}$ is algebraically independent from $r(B \setminus \{\psi\}) \cup \{\overline{\rho}^{\overline{m}}\} \cup \overline{c}$. Similarly, there is a $\psi' = \overline{\rho}^{\overline{m}'} \overline{\theta}^{\overline{m}'}$ such that the function $\overline{\theta}^{\overline{q}}$ is algebraically independent from $r(B \setminus \{\psi'\}) \cup \{\overline{\theta}^{\overline{m}'}\} \cup \overline{c}$.

Moreover, again by Lemma 9.14, for all the possible ψ's $\overline{\rho}^{\overline{q}}$ is algebraically independent from $r(B \setminus \{\psi\}) \cup \{\overline{\theta}^{\overline{m}}\} \cup \overline{c}$ and $\overline{\theta}^{\overline{q}}$ is algebraically independent from $r(B \setminus \{\psi\}) \cup \{\overline{\rho}^{\overline{m}}\} \cup \overline{c}$.

Now, let us extract a maximal algebraically independent set S_0' from B such that S_0' is a set of coordinate functions of $M \cdot r(V)$, similarly to S_0; in other words, we extract a transcendence base among the functions in $r(B)$ that actually appear as coordinates of $M \cdot r(V)$. By hypothesis $|S_0'| = \operatorname{rank} M$.

In any of the above situations, there is a function $\overline{\rho}^{\overline{m}} \overline{\theta}^{\overline{m}}$ such that $\overline{\rho}^{\overline{q}}$ (if $\overline{q}$ is a row of M_1) or $\overline{\theta}^{\overline{q}}$ (if $\overline{q}$ is a row of P_2) is algebraically independent from $r(B \setminus \{\psi\}) \cup \{\overline{\rho}^{\overline{m}}\} \cup \overline{c}$ and from $r(B \setminus \{\psi\}) \cup \{\overline{\theta}^{\overline{m}}\} \cup \overline{c}$. Since (exactly) one of the last two sets contains S_0', this implies $\dim M \cdot \check{V} > \operatorname{rank} M$, a contradiction.

Therefore, $\operatorname{rank} M = 2n$. □

Proposition 9.16. *If $\dim M \cdot \check{V} = \operatorname{rank} M$, and some function in S_0 is not one-dimensional, then all the functions in S_0 are two-dimensional.*

Proof. Let us suppose that we have both kind of functions. By construction, this implies that there are some rows $(\overline{m}, \overline{q})$ in M such that either $\overline{m}$ or $\overline{q}$ are zero, and some where both $\overline{m}$ and $\overline{q}$ are not zero. Note that S_0 is pure.

If $(\overline{m}, 0)$ is a row of M (or $(0, \overline{p})$), then by construction exactly one of the functions $\overline{m} \cdot \overline{x}, \overline{\rho}^{\overline{m}}$ (resp. $\overline{p} \cdot \overline{y}, \overline{\theta}^{\overline{p}}$) is in S_0. Let ψ be the one not contained in S_0. We claim that ψ is contained in the algebraic closure of all the one-dimensional functions in S_0.

Indeed, since $\psi \in \mathrm{acl}(S_0)$, but it is not constant by absolute freeness, there must be at least one function $\chi \in S_0$ such that ψ is interalgebraic with χ over $S_0 \setminus \{\chi\}$. But this implies that $r(\psi)$ is interalgebraic with $r(\chi)$ over $r(S_0 \setminus \{\chi\})$; in particular, χ is one-dimensional too. Applying this argument to all the possible χ's we obtain our claim.

However, this implies that if M' is the submatrix of M of all the rows $(\overline{m}, \overline{q})$ of M such that either $\overline{m}$ or $\overline{q}$ is zero, we have that $\dim M' \cdot \check{V} = \mathrm{rank} M'$. But all the coordinate functions are one-dimensional on $M' \cdot \check{V}$, hence we have $\mathrm{rank} M' = 2n$. This implies that *all* the functions in S_0 are one-dimensional, a contradiction.

Therefore, all the functions in S_0 are two-dimensional. □

And then the last observation.

Proposition 9.17. *If $\dim M \cdot \check{V} = \mathrm{rank} M$, and all the functions in S_0 are two-dimensional, then M is of the form*

$$M = \begin{pmatrix} N & Q \end{pmatrix}$$

where N, Q are two matrices in $\mathcal{M}_{n,n}(\mathbb{Z})$ of maximum rank.

Proof. Since the functions in S_0 are all two-dimensional, the matrix M is of the following form:

$$M = \begin{pmatrix} N & Q \end{pmatrix},$$

where N and Q are some matrices in $\mathcal{M}_{k,n}(\mathbb{Z})$ of maximum rank k.

Let us consider the matrix

$$M' := \begin{pmatrix} N & 0 \\ 0 & Q \end{pmatrix}.$$

Obviously, $\mathrm{rank} M' = 2k$.

Clearly, there is a surjective algebraic map $M' \cdot \check{V} \to M \cdot \check{V}$ which is a bijection when restricted to the realizations $M' \cdot r(V) \to M \cdot r(V)$. In other words, we could say $r(M \cdot r(V)) = M' \cdot r(V)$. This implies that the dimension of $M' \cdot r(V)$ is $2k$.

But this means that $\dim M' \cdot V = \mathrm{rank} M'$, and by Proposition 9.15, $\mathrm{rank} M' = 2k = 2n$. Therefore, $k = n$, and we are done. □

This ends the proof of Theorem 9.1.

Proof of Theorem 9.1. By Propositions 9.2, 9.3 and 9.9, $\check{V}$ is absolutely free, absolutely irreducible and rotund.

Let $A \cdot M$ be the matrix obtained in Proposition 9.4. By Proposition 9.16, the coordinate functions of $A \cdot M \cdot r(V)$ are either one-dimensional or two dimensional. In the former case, by Proposition 9.15 $A \cdot M$ is invertible, and thus M is invertible two.

In the latter case, by Proposition 9.17 the matrix $A \cdot M$ has the desired form, and thus M has the desired form too. □

10. Solutions and roots on the $\mathbb{G}$-restrictions

As anticipated in Section 7, we need some kind of alternative version of Proposition 7.6 to work with dense sets of real generic solutions. In order to do this, we produce a suitable generalization taking into accounts the $\mathbb{G}$-restrictions. First of all, we introduce some other technical definitions.

Definition 10.1. An *open subfamily* of $\mathcal{R}(V)$ is a collection of subsets $\mathcal{U} := \{\mathcal{U}(W)\}_{W\in\mathcal{R}(V)}$ such that $\mathcal{U}(W) \subset W$ is open in W w.r.t. the order topology.

We extend the usual set-theoretic operations to the open subfamilies: the union of two or more open subfamilies is the subfamily of the union of the respective open sets, one subfamily $\mathcal{U}$ is contained in another $\mathcal{U}'$ if for each $W \in \mathcal{R}(V)$ we have $\mathcal{U}(W) \subset \mathcal{U}'(W)$, etc. etc.

Definition 10.2. A family $\mathcal{R}(V)$, for V defined over $\overline{c}$, is *densely solved* in K_E w.r.t. an open subfamily $\mathcal{U}$ if for all $W \in \mathcal{R}(V)$ there is an infinite set of solutions of W really algebraically independent over $\operatorname{acl}(\overline{c})$ which is dense in $\mathcal{U}(W)$ w.r.t. the order topology.

We say that $\mathcal{R}(V)$ is *densely solved* in K_E if it is densely solved w.r.t. the trivial open subfamily $\mathcal{R}(V)$.

Again, this definition does not depend on $\overline{c}$. Indeed, if we use another $\overline{d}$ by Proposition 5.3 a set of algebraically independent points remains algebraically independent when passing from $\overline{c}$ to $\overline{d}$, up to removing a finite set of points. As there are no isolated points in any of the varieties $W \in \mathcal{R}(V)$, the set of solutions remains dense after removing a finite set.

Proposition 10.3. *If $W \in \mathcal{R}(V)$, then $\check{W} \in \mathcal{R}(\check{V})$.*

Proof. There are $p, q \in \mathbb{Z}^\times$ such that $q \cdot W = p \cdot V$. Taking the realization we obtain $q \cdot r(W) = p \cdot r(V)$; taking the Zariski closure, $q \cdot \check{W} = p \cdot \check{V}$. □

The following is the 'right' version of Proposition 7.6 for densely solved families.

Proposition 10.4. *Let $V \subset \mathbb{G}^n$ be a rotund variety and K_E such that $\sigma\circ E = E\circ\sigma$. Let $N, Q \in \mathcal{M}_{n,n}(\mathbb{Z})$ be two square integer matrix of maximum rank, $\overline{z} \in \operatorname{dom}(E)^n$, and $X := \begin{pmatrix} N & Q \end{pmatrix} \cdot \check{V} \oplus \langle \overline{z}; E(\overline{z})\rangle$.*

If $\dim X = \dim V$, then there exists an open subfamily $\mathcal{U}$ of $\mathcal{R}(X)$ such that $\mathcal{R}(V)$ is densely solved if and only if $\mathcal{R}(X)$ is densely solved w.r.t. $\mathcal{U}$.

Proof. For each $W \in \mathcal{R}(V)$ we have $\check{W} \in \mathcal{R}(\check{V})$; in particular, there are $p, q \in \mathbb{Z}^\times$ such that $M \cdot \check{W} \oplus \langle \frac{p}{q}\overline{z}; E(\frac{p}{q}\overline{z})\rangle \in \mathcal{R}(X)$. Let Y be $M \cdot \check{W} \oplus \langle \frac{p}{q}\overline{z}; E(\frac{p}{q}\overline{z})\rangle$.

For brevity, let $\psi_W : W \to Y$ be the map

$$\psi_W(P) := \begin{pmatrix} N & Q \end{pmatrix} \cdot r(P) \oplus \langle \frac{p}{q}\overline{z}; E(\frac{p}{q}\overline{z})\rangle.$$

Let $\tilde{N}, \tilde{Q}$ be two integer matrices such that $\tilde{N} \cdot N = \tilde{Q} \cdot Q = k \cdot \mathrm{Id}$ for some $k \in \mathbb{N}^\times$. We define $\tilde{\psi}_W : \psi_W(W) \to W$ as

$$\tilde{\psi}_W(R) := \begin{pmatrix} \tilde{N} & 0 \\ 0 & \tilde{Q} \end{pmatrix} \cdot r\left(\psi_W(P) \oplus \langle -\frac{p}{q}\overline{z}; E(-\frac{p}{q}\overline{z})\rangle\right).$$

Seen as a map between $r(W)$ and $r(Y)$, both are semi-algebraic map. We claim that ψ_W is finite-to-one onto its image. Indeed, if $\psi_W(P)$ is a point in the image, then

$$\tilde{\psi}_W(\psi_W(P)) = k \cdot r(P) = r(k \cdot P).$$

Since there are finitely many points P' such that $k \cdot P' = k \cdot P$, and r is injective, the map ψ_W is finite-to-one.

This implies that $o\text{−}\dim(\psi_W(W)) = o\text{−}\dim(Y)$, where by "$o\text{−}\dim$" we denote the o-minimal dimension over R. In particular, by o-minimality there is an open subset U_Y of Y such that $U_Y \subset \psi_W(W)$ and

$$o\text{−}\dim(\psi_W(W) \setminus U_Y) < o\text{−}\dim(\psi_W(W)).$$

In particular, $\psi_W^{-1}(U_Y)$ is an open subset of V such that

$$o\text{−}\dim(W \setminus \psi_W^{-1}(U_Y)) < o\text{−}\dim(W).$$

For each Y, we have selected an open subset U_Y; for the remaining varieties in $\mathcal{R}(X)$, we take the empty set. We claim that the resulting open subfamily $\mathcal{U}$ is the desired one.

From now on, let $\overline{c}$ be a defining tuple for $\check{V}$ containing $r(\langle \overline{z}; E(\overline{z})\rangle)$. In particular, $\overline{c}$ also defines both V and X.

The left-to-right direction is clear: since ψ_W is continuous, algebraic, defined over $\overline{c}$, and finite-to-one, it sends really algebraically independent dense sets to really algebraically independent sets dense in the image; in particular, the image of the solutions in W through ψ_W will be a dense, algebraically independent set w.r.t. U_Y. As the family $\mathcal{U}$ is composed exactly by the U_Y's, the conclusion follows.

For the right-to-left we proceed as above. The map $\tilde{\psi}_W$, for $P \in U_Y$, is such that $\tilde{\psi}_W \circ \psi_W$ is exactly $k \cdot \mathrm{Id}$. Hence it is a finite-to-one algebraic continuous map, so as above it preserves really algebraically independent dense sets over $\overline{c}$.

In particular, if there is a dense set of really algebraically independent points in U_Y, then there is a corresponding dense set of really algebraically independent points in $\tilde{\psi}_W(U_Y)$. However, this set is exactly $k \cdot \psi_W^{-1}(U_Y)$. Since $\psi_W^{-1}(U_Y)$ has complement of o-minimal dimension strictly smaller than W, and the local dimension of W is always $o\text{−}\dim(W) = 2 \cdot \dim(W)$, we have that $\psi_W^{-1}(U_Y)$ is dense in W; hence, its multiple $k \cdot \psi_W^{-1}(U_Y)$ is dense in $k \cdot W$.

In particular, the image of the solutions through $\tilde{\psi}_W$ is dense in $k \cdot W$. But for all $W \in \mathcal{R}(V)$ there is a W' such that $k \cdot W' = W$; therefore, if all the open sets in the family $\mathcal{U}$ contains a dense set of really algebraically independent solutions, the same is true for all the varieties in $\mathcal{R}(V)$. □

11. $K_{E_{|K|}}$ is a Zilber field

We finally proceed to the full verification that all the axioms listed in Section 2 are satisfied in the E-field $K_{E_{|K|}}$ produced in Section 3.

Proposition 11.1. *$K_{E_{|K|}}$ satisfies (ACF$_0$), (E), (LOG), (SEC).*

Proof. The axiom (ACF$_0$) is trivially true, as K is algebraically closed and has characteristic 0.

At each substep, we define E on some new elements $\mathbb{Q}$-linearly independent over the previous domain; hence, the function is well-defined and it satisfies the equation $E(x+y) = E(x) \cdot E(y)$. Moreover, since we run over the whole enumeration $\{\alpha_j\}$ of $R \cup iR$, and $R + iR = K$, then $\mathrm{dom}(E_{|K|}) = K$. Therefore $K_{E_{|K|}}$ satisfies (E).

Similarly, we run over the whole enumeration $\{\beta_j\}$ of $R_{>0} \cup \mathbb{S}^1(K)$, and $K^\times$ is $R_{>0} \cdot \mathbb{S}^1(K)$, so $E_{|K|}(K) = K^\times$, i.e., $K_{E_{|K|}}$ satisfies (LOG).

Every simple variety V appears in the sequence $\{V_j\}$, so for some finite $\overline{c}$ there are infinitely many $\overline{z}$ such that $\langle \overline{z}; E_{|K|}(\overline{z})\rangle \in V_j$, and they are algebraically independent over $\overline{c}$. By Fact 5.1, $K_{E_{|K|}}$ satisfies (SEC). □

Note that moreover the set of the solutions of simple varieties is dense, so that also axiom (DEN) of Section 4 is satisfied.

Proposition 11.2. *For all $j \geq -1$, $\ker(E_j) = i\omega\mathbb{Z}$. In particular, $K_{E_{|K|}}$ satisfies (STD) and $\ker(E_{|K|}) = i\omega\mathbb{Z}$.*

Proof. The kernel of E_{-1} is exactly $i\omega\mathbb{Z}$ at the base step. We claim that for any of the finite operations $\ker(E) = \ker(E')$. It is clear that $\ker(E) \subset \ker(E')$, so it is sufficient to prove the other inclusion.

DOMAIN. If $\alpha \in D$, the conclusion is clear, so we may assume that $\alpha \notin D$. Let us suppose that in $\mathrm{dom}(E')$ there is an element x such that $E'(x) = 1$. By definition of E', it means that there is a $z \in D$ and a rational number $\frac{p}{q}$ such that $E'(z + \frac{p}{q}\alpha) = E(z) \cdot \beta^{p/q} = 1$. This means that $\beta^p = E(z)^{-q} \in E(D)$, but β is transcendental over $E(D)$, so we must have $p = 0$. This implies $x = z \in D$, and in turn $x \in \ker(E)$.

IMAGE. If $\beta \in E(D)$, the conclusion is again clear, so we may assume that $\beta \notin E(D)$. As above, if $x \in \mathrm{dom}(E')$ is such that $E'(x) = 1$, then $E(z) \cdot \beta^{p/q} = 1$ for some $z \in D$ and some rational number p/q. However, if $p \neq 0$ this implies $\beta = E(-\frac{q}{p}z)$, i.e., $\beta \in E(D)$, a contradiction, so we must have $p = 0$. This implies again $x = z \in D$, so $x \in \ker(E)$.

SOLUTIONS. This operation can be seen as a sequence of extensions, each one made by extending E using a generic point of a variety of the form $\check{V}$. By Theorem 9.1, if V is absolutely free, then $\check{V}$ is absolutely free. By Fact 5.2, $\ker(E) = \ker(E')$.

Since we have the equality at all the finite operations, the equality holds also at the limit operation:

LIMIT. $\ker(E') = \bigcup_{k'<j} \ker(E_{k'}) = \ker(E_k)$ for any $k < j$.

In particular, for all $j \leq |K|$, $\ker(E_j) = \ker(E_{-1}) = i\omega\mathbb{Z}$. □

Proposition 11.3. *For all $j \geq -1$, K_{E_j} satisfies (SP). In particular, $K_{E_{|K|}}$ satisfies (SP).*

Proof. The axiom (SP) is satisfied at the base step $K_{E_{-1}}$. We claim that for any of the basic operation $K_E \leq K_{E'}$.

DOMAIN. If $\alpha \in D$, the conclusion is clear, so we may assume that $\alpha \notin D$. But this holds:

$$\mathrm{tr.deg.}(\alpha, E'(\alpha)/D \cup E(D)) \geq \mathrm{tr.deg.}_{F(\alpha)}(\beta) = 1 = \mathrm{lin.d.}(\alpha/D),$$

hence $\delta'(\alpha/D) \geq 0$, i.e., $K_E \leq K_{E'}$.

IMAGE. If $\beta \in E(D)$, the conclusion is again clear, so we may assume that $\beta \notin E(D)$. As above,

$$\mathrm{tr.deg.}(\alpha, E'(\alpha)/D \cup E(D)) \geq \mathrm{tr.deg.}(\alpha/F(\beta)) = 1 = \mathrm{lin.d.}_D(\alpha),$$

hence $K_E \leq K_{E'}$.

SOLUTIONS. This operation can be seen as a sequence of extensions, each one made by extending E using a generic point of a variety of the form $\check{V}$. By Theorem 9.1, if V is rotund, then $\check{V}$ is rotund. By Fact 5.2, $K_E \leq K_{E'}$.

Since the limit of strong extensions is a strong extension,

LIMIT. $K_{E_k} \leq K_{E'}$ for any $k < j$.

This implies that $K_{E_{-1}} \leq K_{E_j}$, so by Fact 5.7 K_{E_j} satisfies (SP). □

Proposition 11.4. *For all $j \geq -1$, $\sigma \circ E_j = E_j \circ \sigma$.*

Proof. Indeed, by construction we have $E_j(R) \subset R_{>0}$ and $E_j(iR) \subset \mathbb{S}^1(K)$; by Proposition 3.1, this implies that $\sigma \circ E = E \circ \sigma$. □

Proving (CCP) is much more difficult. Let D_j be the domain of the function E_j, and F_j the field generated by $D_j, E(D_j)$, for $j \leq |K|$.

Proposition 11.5. *For all $j \leq |K|$, K_{E_j} satisfies (CCP). In particular, $K_{E_{|K|}}$ satisfies (CCP).*

Proof. It is clear that $K_{E_{-1}}$ satisfies (CCP), as $\mathrm{dom}(E_{-1}) = \omega\mathbb{Q}$ is countable. We want to prove that (CCP) holds on K_{E_j} by induction.

First of all, for all j there is a finite or countable set B_j such that $D_{j+1} = \mathrm{span}_{\mathbb{Q}}(D_j \cup B_j)$. By Lemma 6.2, if K_{E_j} satisfies (CCP), then $K_{E_{j+1}}$ satisfies (CCP). We claim the induction works also at limit ordinals.

Let j be a limit ordinal such that for all $k < j$, K_{E_k} satisfies (CCP). By Proposition 6.1, in order to prove (CCP) for K_{E_j} it is sufficient to verify that for any perfectly rotund variety defined over D_j, the number of generic solutions is at most countable. We may restrict to absolutely irreducible varieties by taking them defined over $\mathrm{acl}(D_j)$.

Let $X(\overline{c}) \subset \mathbb{G}^n$ be a perfecly rotund variety with $\overline{c} \subset \mathrm{acl}(D_j)$. If $\overline{x} \in D_j^n$ is a generic solution of $X(\overline{c})$ in K_{E_j}, then there is a smallest $k+1$ such that $\overline{x} \in D_{k+1}^n$ and $\overline{c} \subset \mathrm{acl}(D_k)$. Note that we can restrict to ordinals of the form $k+1$, as they can only be successors. Let $\Lambda \subset j$ be the subset composed by such ordinals $k+1$.

We claim that Λ has countable cofinality. Since the generic solutions of $X(\overline{c})$ in K_{E_λ} are countably many for each $\lambda \in \Lambda$, and the generic solutions in K_{E_j} are the union of the solutions at the steps λ, its cofinality would imply that there are countably many solutions at K_{E_j}. Therefore K_{E_j} would satisfy (CCP_2), and in turn (CCP).

Let $\overline{x}$ be a new generic solution of $X(\overline{c})$ contained in $D_{k+1} \setminus D_k$. First of all, we claim that the solution $\overline{x}$ cannot appear as a consequence of one of the two operations DOMAIN and IMAGE, during the first three substeps 1a, 1b and 1c.

For both operations, let D be the domain before the operation, and (α, β) the new point we are adding to the graph of E. Let D' be the new domain $\mathrm{span}_{\mathbb{Q}}(D \cup \{\alpha\})$. Let F be the field generated by $D, E(D)$. By hypothesis, $\overline{c} \subset \mathrm{acl}(F)$.

DOMAIN, IMAGE. The vector $\overline{x}$ must be of the form $\overline{z} + \alpha \cdot \overline{m}$, where $\overline{m}$ is a vector in $\mathbb{Z}^n \setminus \{0\}$ and $\overline{z} \in D^n$. By using a square integer matrix M of maximum rank, we may transform the solution to one of the form

$$\langle M \cdot \overline{z} + \alpha \cdot m \cdot \overline{e}_1; E(M \cdot \overline{z} + \alpha \cdot m \cdot \overline{e}_1)\rangle \in M \cdot X(\overline{c}),$$

where m is some integer and $\overline{e}_1$ is the vector $(1, 0, \ldots, 0)$.

The variety $M \cdot X(\overline{c})$ is still perfectly rotund. We distinguish two cases.

If $n \geq 2$, let $\overline{e}_j$ be the vectors that are 1 on the j-th coordinate, and 0 on the rest. Let N be the matrix which is the identity on $\overline{e}_j$ for $j > 1$, and the zero map on $\overline{e}_1$. Since $M \cdot X$ is perfectly rotund, then $\dim(N \cdot M \cdot X) = n$, hence the point $\langle N \cdot M \cdot \overline{z}; E(N \cdot M \cdot \overline{z})\rangle$ has transcendence degree n over $\overline{c}$. In particular,

$$\mathrm{tr.deg.}_{\overline{c}}\langle N \cdot M \cdot \overline{z}; E(N \cdot M \cdot \overline{z})\rangle = \mathrm{tr.deg.}_{\overline{c}}\langle M \cdot \overline{z} + \alpha \cdot m \cdot \overline{e}_1; E(M \cdot \overline{z} + \alpha \cdot m \cdot \overline{e}_1)\rangle.$$

This implies that α and $\beta = E(\alpha)$ are both algebraic over $\langle \overline{z}; E(\overline{z})\rangle \cup \overline{c}$, and in particular over $F(\overline{c}) \subset \mathrm{acl}(F)$. However, we have $\mathrm{tr.deg.}_F(\alpha, \beta) \geq 1$, a contradiction.

If $n = 1$, then $\dim X(\overline{c}) = 1$, and the new point is of the form $z + \alpha \cdot m$. Since the variety is absolutely free, we have that $z + \alpha \cdot m$ and $E(z) \cdot \beta^m$ are both transcendental over $\overline{c}$, but interalgebraic over $\overline{c}$; in other words, there is an irreducible polynomial over $\overline{c}$ where both of them appears. In particular, they are interalgebraic over F. However, by construction we either have $\mathrm{tr.deg.}_{F(\alpha)}(\beta) = 1$ or $\mathrm{tr.deg.}_{F(\beta)}(\alpha) = 1$, a contradiction.

The only remaining possibility is that the solution $\overline{x}$ appears during the substep 1d. In this case the discussion is a bit more complicated.

SOLUTIONS. This operation is a sequence of multiple operations. Let us suppose that the solution $\overline{x}$ appears when we add the point $\langle \overline{\alpha}; \overline{\beta}\rangle \in \check{V}$ to the graph of the exponential function, for some simple variety $V \subset \mathbb{G}^m$. As above, let D be

the domain of the exponential function before adding the point $\langle\overline{\alpha};\overline{\beta}\rangle$, and let $D' := \operatorname{span}_{\mathbb{Q}}(D\cup\overline{\alpha})$ be the domain after. The vector $\overline{x}$ must be of the form $\overline{z}+M\cdot\overline{\alpha}$, for some matrix $M \in \mathcal{M}_{n,2m}(\mathbb{Q}) \setminus \{0\}$, and $\overline{z} \in D$. Let $F := \mathbb{Q}(D, E(D))$.

For now, let us assume that M is an integer matrix.

Under the above assumptions, $\text{tr.deg.}_F(\overline{\alpha}, E(\overline{\alpha})) = \dim \check{V} = 2m$. Moreover, for any matrix P we have $\text{tr.deg.}_F(P\cdot\overline{\alpha}, E(P\cdot\overline{\alpha})) \geq \text{rank}P$.

Now, let N be an invertible matrix with integer coefficients such that the first rows of $N\cdot M$ forms a matrix Q of maximum rank equal to $\text{rank}M$, and that the remaining rows are zero. Clearly, the point $\langle N\cdot\overline{z}+N\cdot M\cdot\overline{\alpha}; E(N\cdot\overline{z}+N\cdot M\cdot\overline{\alpha})\rangle$ is generic for $N\cdot X(\overline{c})$, which is again a simple variety.

Let $N\cdot\overline{z} = \overline{z}'\overline{z}''$, where $\overline{z}'$ is formed by the first $\text{rank}M$ coordinates and $\overline{z}''$ by the remaining $(n-\text{rank}M)$ ones. Let us suppose that $n > \text{rank}M$. By simpleness of $N\cdot X(\overline{c})$, we have $\text{tr.deg.}_{\overline{c}}(\overline{z}'', E(\overline{z}'')) > (n-\text{rank}M)$.

In particular, we also have $\text{tr.deg.}_{\overline{c},\overline{z}'',E(\overline{z}'')}(\overline{z}'+Q\cdot\overline{\alpha}, E(\overline{z}'+Q\cdot\overline{\alpha})) < \text{rank}M$. However, this contradicts the fact that $\text{tr.deg.}_F(Q\cdot\overline{\alpha}, Q\cdot E(\overline{\alpha})) \geq \text{rank}Q = \text{rank}M$. This implies that $n = \text{rank}M$.

The resulting situation is that $\langle\overline{z}+M\cdot\overline{\alpha}; E(\overline{z}+M\cdot\overline{\alpha})\rangle$ is a generic point of $X(\overline{c})$ *over* F, while it is also a generic point of $M\cdot\check{V}\oplus\langle\overline{z};E(\overline{z})\rangle$ over F. This immediately implies the equality $M\cdot\check{V}\oplus\langle\overline{z};E(\overline{z})\rangle = X$. Moreover, $\dim V = \dim X$.

In particular, we also have

$$\text{tr.deg.}_F(\overline{z}+M\cdot\overline{\alpha}, E(\overline{z}+M\cdot\overline{\alpha})) = \text{tr.deg.}_{F(\overline{c})}(M\cdot\overline{\alpha}, E(M\cdot\overline{\alpha})) = \text{rank}M.$$

By Theorem 9.1, M is either invertible or of the form $\begin{pmatrix} N & Q \end{pmatrix}$, with both N and Q invertible of rank $n = m$. In the former case, we would obtain that $\check{V}$ is simple, a contradiction. Hence, M must be of the latter form, and V must be perfectly rotund.

In particular, by Proposition 10.4 there is an open subfamily $\mathcal{U}_{V,M,\overline{z}}$ such that $\mathcal{R}(V)$ is densely solved if and only if $\mathcal{R}(X)$ is densely solved w.r.t. $\mathcal{U}_{V,M,\overline{z}}$.

If M is not an integer matrix, let l be an integer such that $l\cdot M$ is an integer matrix; the above argument applied to $l\cdot M$, $l\cdot\overline{z}$ and $l\cdot X$ implies that $\mathcal{R}(V)$ is densely solved if and only if $\mathcal{R}(l\cdot X)$ is densely solved w.r.t. $\mathcal{U}_{V,l\cdot M,l\cdot\overline{z}}$. As $\mathcal{R}(l\cdot X) = \mathcal{R}(X)$, this is just like the above conclusion.

Now, for each of the varieties such that the above situation happens, i.e., for each $\lambda\in\Lambda$, we choose, among the possibilities found above, one matrix M and one vector $\overline{z}$ such that $\mathcal{R}(V_\lambda)$ is densely solved if and only if $\mathcal{R}(X)$ is densely solved w.r.t. the family $\mathcal{U}_\lambda := \mathcal{U}_{V_\lambda,M,\overline{z}}$.

By second-countability of the order topology, we can extract an at most countable subsequence $\{\mathcal{U}_{\lambda_p}\}_{p<f\leq\omega}$, for some fixed f, such that for each $Y\in\mathcal{R}(X)$, the union $\bigcup_{\lambda\in\Lambda}\mathcal{U}_\lambda(Y)$ is covered by $\bigcup_p\mathcal{U}_{\lambda_p}(Y)$. We claim that the subsequence (λ_p) is cofinal in Λ.

Indeed, let us take a variety V_λ with $\lambda\in\Lambda$, and let us suppose by contradiction that $\lambda > \lambda_p$ for all $p < f$. We know that $\mathcal{R}(V_\lambda)$ is densely solved if and only if $\mathcal{R}(X)$ is densely solved w.r.t. $\mathcal{U}_\lambda$. We claim that $\mathcal{R}(X)$ is densely solved w.r.t. $\mathcal{U}_\lambda$ *before* the step λ.

Indeed, if $U\subset Y\in\mathcal{R}(X)$ is an open set of the family $\mathcal{U}_\lambda$, then U is covered by the union of some open sets U_p, with $U_p\in\mathcal{U}_{\lambda_p}$. However, by construction, after step λ_p, and in particular at step λ, the open sets U_p contain a dense set of really algebraically independent solutions. In particular, at step λ the open set U contains a dense set of really algebraically independent solutions. This means that at step λ the family $\mathcal{R}(X)$ is densely solved w.r.t. $\mathcal{U}_\lambda$, and in turn $\mathcal{R}(V_\lambda)$ is densely solved.

But this actually implies that at step λ we *do not* add new solutions to V_λ, a contradiction. This implies that $(\lambda_p)_{p<\omega}$ is cofinal in Λ.

The set of the generic solutions of $X(\overline{c})$ contained in K_{E_j} is the union of the solutions contained in K_{E_λ} for $\lambda \in \Lambda$; by cofinality, this is just the union of the solutions contained in $K_{E_{\lambda_p}}$ for $p < \omega$. But this is an at most countable union of countable sets, hence $X(\overline{c})$ has at most countably many generic solutions in K_{E_j}.

By induction, this proves that for all $j \leq |K|$, K_{E_j} satisfies (CCP). □

We have obtained our proof:

Proof of Theorem 1.2. By Propositions 11.1, 11.2, 11.3 and 11.5, $K_{E_{|K|}}$ is a Zilber field, and by Proposition 11.4, σ commutes with $E_{|K|}$, hence it is an involution of $K_{E_{|K|}}$. Moreover, the kernel of $E_{|K|}$ is exactly $i\omega\mathbb{Z}$.

Taking $E = E_{|K|}$, we obtain the desired result. □

Remark 11.6. By construction, each simple variety has a dense set of solutions. This proves the existence of at least one model of cardinality $2^{\aleph_0}$ for Theorem 4.1, and the existence of the other models follow by the argument given in Section 4.

Remark 11.7. Our construction is potentially abundant for two reasons. First, we add "real generic" solutions to rotund varieties, and it is not clear if a Zilber field with an involution must satisfy this condition.

Moreover, in the operation SOLUTIONS we check if the family $\mathcal{R}(V)$ is densely solved before proceeding. Actually, it would be sufficient to check if $\mathcal{R}(V)$ is completely solved, without looking at density. This would open the possibility for involutions where the sets of the solutions are not always dense, but it is unclear what could happen in this situation.

12. Further results

The general strategy used in our construction can be useful also for showing other properties of Zilber fields.

Here we use it to obtain a full classification of which partial E-fields can be embedded into Zilber fields. It is immediate to see that in order to be embeddable, a partial E-field must satisfy (SP), (CCP), and the kernel must be either trivial or cyclic; we prove that this is also sufficient. This was already known, but it has never been explicitly stated. A corollary of this statement is that if Schanuel's Conjecture is true, then we know at least that $\mathbb{C}_{\exp}$ embeds into $\mathbb{B}$.

Moreover, we show that if we replace the full axiom (SEC) with a weaker version, stating that just certain simple varieties have solutions (namely, curves in $\mathbb{G}^1$), then we can create a function E such that $E_{\restriction K^\sigma}$ is *monotone*. It has been proven in [1, 6] that if Schanuel's Conjecture is true, then the weaker axiom holds on $\mathbb{C}_{\exp}$.

If we go further and drop completely axiom (SEC), then we can obtain a *continuous* E. The study of these cases shows quite explicitly where the general construction fails at producing an order-preserving or a continuous E.

By the embeddability result, we also find that the resulting fields embed into all the Zilber fields of equal and larger cardinality. This is analogue to the result by Shkop [7], who proved that there are several real closed fields inside Zilber fields such that the restriction of the exponential to the real line is monotone.

12.1. **Embeddability.** If we drop the involution σ, the construction of Section 3 gives a general method to directly build Zilber fields. As a bonus, we can actually build a Zilber field extending a given partial exponential function satisfying certain

properties. A direct construction of this kind is studied in [3], but without the relevant proofs for the uncountable case.

Our approach is indeed similar to the one of [3], with just some differences. We do things in a different order, and we adopt some complications in order to make it easier to verify (CCP). Some of the complications could be probably avoided, such as using system of roots, but at the expense of a more difficult proof.

The result we obtain is the following.

Theorem 12.1. *Let K_E be a partial E-field satisfying (SP) and (CCP).*

If $\ker(E) = \{0\}$ *or* $\ker(E) = i\omega\mathbb{Z}$ *for some* $\omega \in K^\times$*, then there is a strong embedding* $K_E \leq L_{E'}$ *into a Zilber field* $L_{E'}$*.*

The converse is clearly true: if a partial E-field is (strongly) embedded into a Zilber field, then it satisfies (SP) and (CCP), and its kernel is either trivial or cyclic.

As $\mathbb{C}_{\exp}$ satisfies (CCP), this shows that Schanuel's Conjecture is true if and only if $\mathbb{C}_{\exp}$ embeds into $\mathbb{B}$.

In order to prove Theorem 12.1 we proceed as in Section 3: we enlarge the field K to some bigger field L and we define E' by back-and-forth, extending E.

First of all, we choose an algebraically closed field $L \supset K$ whose cardinality is strictly greater than the cardinality of K. If $\ker(E)$ is non-trivial, we fix $E_{-1} := E$. Otherwise, we choose an arbitrary $\omega \in L$ transcendental over K, a coherent system of roots of unity $(\zeta_q)_{q\in\mathbb{N}^\times}$, and we define $E_{-1}(x+\frac{p}{q}\omega) = E(x)\cdot\zeta_q^p$, with $x \in \mathrm{dom}(E)$.

$L_{E_{-1}}$ is our new base step. The rest of the construction of the sequence $(E_j)_{j\leq|L|}$ is the same as Section 3, just by dropping all the references to σ, with the obvious changes in the enumerations, in the operations and in the construction. Here we show explicitly just the most sensible change, which is in the operation **solutions**:

solutions': We start with the family $\mathcal{R}(V)$ associated to an absolutely irreducible variety V, such that for some finite tuple $\overline{c} \subset D$, all the varieties $W \in \mathcal{R}(V)$ are defined over $\mathrm{acl}(\overline{c}) \cap D$. If $\mathcal{R}(V)$ is completely solved, we proceed to the next step. Otherwise we do the following.

Let $\mathcal{R}(V)$ be enumerated as $(W_k)_{k<\omega}$, and let $E_{0,0} := E$. We define by double induction on $k, l < \omega$ some new temporary functions $E_{k,l}$.

At step $(k,0)$ we are given the function $E_{k,0}$. At the step (k,l), we take a point $((\alpha_1,\beta_1),\ldots,(\alpha_n,\beta_n)) \in W_k$ generic over $\mathrm{dom}(E_{k,l}), \mathrm{im}(E_{k,l})$, we fix a system of roots $\beta_j^{1/q}$ of β_j, and we define

$$E_{k,l+1}(z + \frac{p_1}{q_1}\alpha_1 + \cdots + \frac{p_n}{q_n}\alpha_n) := E_{k,l}(z)\cdot\beta_1^{p_1/q_1}\cdot\cdots\cdot\beta_n^{p_n/q_n}.$$

We define then $E_{k+1,0} := \bigcup_{l<\omega} E_{k,l}$.

At the end, we define $E' := \bigcup_{k<\omega} E_{k,0}$.

The proof that the final structure $L_{E_{|L|}}$ is a Zilber field is also quite similar, with another sensible difference in managing the operation solutions'. We sketch the modified proof here.

Proof of Theorem 12.1. We need to prove that $L_{E_{|L|}}$ is a Zilber field.

First of all, we observe that $K_E \leq L_{E_{-1}}$, and that (CCP) holds on $L_{E_{-1}}$. Then axioms (ACF_0), (E), (LOG), (SEC), (STD) and (SP) can be verified by repeating almost identically the proofs of Propositions 11.1, 11.2 and 11.3.

In order to verify (CCP), we need to repeat the proof of Proposition 11.5 with one essential change: since in solutions' we are adding generic point to *simple* varieties rather than their $\mathbb{G}$-restrictions, we can use the stronger Proposition 7.6 in place of Proposition 10.4. This is sufficient to prove that the set Λ has cardinality

at most 1, rather than proving that it has countable cofinality. This provides again the induction at limit ordinals.

Therefore, $L_{E_{|L|}}$ is a Zilber field. □

Note that the use of Proposition 7.6 instead of Proposition 10.4, and the fact that in the operation SOLUTIONS' we do not need a dense set of solutions, let the induction work also on cardinalities greater than $2^{\aleph_0}$.

12.2. **A monotone $E_{\restriction K^\sigma}$ and a continuous E (without (SEC)).** Our construction fails at producing an exponential function E such that E is continuous, and it is not even capable to make the restriction $E_{\restriction K^\sigma}$ increasing.

In order to see why, we present first an example construction where E is increasing, at the price of dropping the axiom (SEC) from the final structure. Not everything is lost, however, as we manage to verify a partial instance of (SEC) which we call "(1-SEC)". This example makes evident where our technique fails in producing order-preserving exponential functions.

The following axiom is the special instance of (SEC) we manage to verify.

(1-SEC) 1-dimensional Strong Exponential-algebraic Closure: for every absolutely free rotund variety $V \subset \mathbb{G}^1$ irreducible over K, and every tuple $\overline{c} \in K^{<\omega}$ such that V is defined over $\overline{c}$, there is a generic solution of $V(\overline{c})$.

It is known that if Schanuel's Conjecture is true, then (1-SEC) holds on $\mathbb{C}_{\exp}$ [6, 1]. It is not known if Schanuel's Conjecture implies also (SEC) on $\mathbb{C}_{\exp}$.

The construction, with some adaptation, yields the following.

Theorem 12.2. *For all saturated algebraically closed fields K of characteristic 0 there is a function $E : K \to K^\times$ and an involution σ commuting with E such that K_E satisfies (E), (LOG), (STD), (SP), (1-SEC) and (CCP), and $E_{\restriction K^\sigma}$ is a monotone function.*

As in Section 12.1, we need to do some changes to the construction. Here is just a sketch of what we do.

(1) We start with a large saturated model R of $\mathbb{R}_{\mathrm{an}}$, or just of $\mathbb{R}$ equipped with the cosine function restricted to a suitable interval, and its algebraic closure K (rather than a second-countable real closed field and its algebraic closure).
(2) In the operations DOMAIN and IMAGE on R, we exploit the saturation of R to choose the new values so that E remains a monotone function.
(3) We change the operation SOLUTIONS to add solutions just to simple varieties $V \subset \mathbb{G}^1$ *without requiring the solutions to be dense*, as we did in Section 12.1, and we exploit again the saturation to keep E order-preserving.

The fact that we can keep E order-preserving when adding solutions to simple varieties is guaranteed by the following lemma.

Lemma 12.3. *Let $V \subset \mathbb{G}^1$ be a simple variety. If $f : R \to R$ is any partial strictly increasing function with $|\mathrm{dom}(f)| < |R|$, then there is a point $(z, w) \in V$ transcendental over $|\mathrm{dom}(f)|$ such that $f \cup \{(\Re(z), |w|)\}$ is an increasing function.*

Proof. Let us fix $x_1, \dots, x_n$ points in $\mathrm{dom}(f)$. We claim that there is a transcendental point $(z, w) \in V$ such that for some $1 \leq j < n$, $x_j < \Re(z) < x_{j+1}$ and $f(x_j) < |w| < f(x_{j+1})$.

The set $B := \bigcup_{j=0}^{n} \{(x, w) : x_j \leq x \leq x_{j+1},\ f(x_j) \leq w \leq f(x_{j+1})\}$, where we assume $x_0 = -\infty$ and $x_{n+1} = +\infty$, definably disconnects the upper half plane. The range of z on V is K minus finitely many points, and the range of w is $K^\times$ minus finitely many points; hence, the range of $\Re(z)$ is the whole line R, and the range of $|w|$ is $R^\times$. Moreover, the range of $(\Re(z), |w|)$ must be definably connected.

By Theorem 9.1, the o-minimal dimension of $\begin{pmatrix} 1 & 0 \end{pmatrix} \cdot r(V)$ is 2. This implies that the range of $(\Re(z), |w|)$ must intersect B in its *interior* part, hence there are transcendental points in the intersection.

This implies that the partial type we are trying to realize is finitely satisfiable; by saturation, there exists a realization in K. □

Note that once $E_{\restriction R} \cup \{(\Re(z), |w|)\}$ is monotone, the same is true if we extend the function to the rational multiples of $\Re(z)$.

Since we do not require the solutions to be dense, the proof of (CCP) is again different. The following facts shows that the situation is substantially the same as in Section 12.1. Let us introduce an intermediate definition between Definitions 7.2 and 10.2.

Definition 12.4. A family $\mathcal{R}(V)$, with $\overline{c}$ defining $\check{V}$, is *really completely solved* in K_E if for all $W \in \mathcal{R}(V)$ there is an infinite set of solutions of W really algebraically independent over $\operatorname{acl}(\overline{c})$.

The following stronger version of Theorem 9.1 holds.

Proposition 12.5. *Let $V \subset \mathbb{G}^1$ be a simple variety. If $M \in \mathcal{M}_{1,2}(\mathbb{Z})$ is such that* $\dim M \cdot \check{V} = 1$*, then M is of the form*

$$M = \begin{pmatrix} k & \pm k \end{pmatrix}$$

for some integer $k \in \mathbb{Z}$. In particular, the induced map $V \to M \cdot \check{V}$ is surjective.

Proof. By Theorem 9.1, M must be of the form $M = \begin{pmatrix} a & b \end{pmatrix}$ for some non-zero integers a, b, and $\dim V = 1$.

This means that locally the functions $x + iy$ and $ax + iby$ are holomorphic functions of $\rho\theta$ and $\rho^a\theta^b$ respectively. In particular, $(x + i\frac{b}{a}y)$ is locally a holomorphic function of $\rho\theta^{b/a}$. By the Cauchy-Riemann equations in polar coordinates,

$$\frac{\partial y}{\partial \rho} = -\frac{1}{\rho} \cdot \frac{\partial x}{\partial \vartheta} \quad \text{and} \quad \frac{\frac{b}{a}\partial y}{\partial \rho} = -\frac{1}{\rho} \cdot \frac{\partial x}{\frac{b}{a}\partial \vartheta}.$$

This implies $a^2 = b^2$, i.e., $a = \pm b$. Note that in order to define the variable ϑ we need to use some local inverses of the cosine and of the sine functions.

In other words, $M \cdot \check{V}$ is just $\sigma(k \cdot V)$ for some integer k, hence the induced function $V \to M \cdot \check{V}$ actually is $V \to k \cdot V \to \sigma(k \cdot V)$, which is clearly surjective. □

Using surjectivity, we can repeat the proofs of Propositions 7.6 and 10.4 to obtain the following stronger result.

Proposition 12.6. *Let $V \subset \mathbb{G}^n$ be a rotund variety and K_E a partial E-field such that $\sigma \circ E = E \circ \sigma$. Let $N, Q \in \mathcal{M}_{n,n}(\mathbb{Z})$ be two square integer matrix of maximum rank, $\overline{z} \in \operatorname{dom}(E)^n$, and $X := \begin{pmatrix} N & Q \end{pmatrix} \cdot \check{V} \oplus \langle \overline{z}; E(\overline{z}) \rangle$.*

For $W \in \mathcal{R}(V)$, let $Y_W \in \mathcal{R}(X)$ be the variety $\begin{pmatrix} N & Q \end{pmatrix} \cdot \check{W} \oplus \langle \frac{p}{q}\overline{z}; E(\frac{p}{q}\overline{z}) \rangle$ for some $p, q \in \mathbb{Z}^\times$. If for all W the induced map $W \to Y_W$ is surjective, then $\mathcal{R}(V)$ is really completely solved if and only if $\mathcal{R}(X)$ is.

Hence, the proof is much more similar to the one of Section 12.1.

Proof of Theorem 12.2. The proof is the same as the one of Theorem 12.1, where we replace the use of Proposition 7.6 with Proposition 12.6. In particular, we prove again that Λ has cardinality 1 rather than having countable cofinality.

After having produced a Zilber field L_E on the algebraic closure of R, we reduce the cardinality by taking the closure of some sets of exponentially-algebraically independent elements of R. □

Note that since the resulting K_E is an E-field satisfying (STD), (SP) and (CCP), by Section 12.1 it embeds into a Zilber field of the same dimension.

If we drop also (1-SEC), then it is easy to produce a *continuous* function E.

Theorem 12.7. *For all saturated algebraically closed fields K of characteristic 0 there is a function $E : K \to K^\times$ and an involution σ commuting with E such that K_E satisfies (E), (LOG), (STD), (SP), and (CCP), and E is a continuous function with respect to the topology induced by σ.*

The trick is again to start with a saturated real closed field R, and exploit the saturation in the operations DOMAIN and IMAGE: we make sure at once that $E : K^\sigma \to K^\sigma$ is monotone and that $E : [0, \omega) \to \mathbb{S}^1(K)$ moves 'counterclockwise'. This is sufficient to obtain that E is continuous.

As there is no operation SOLUTIONS in this case, the axioms (SP) and (CCP) are even easier to verify. Again, the resulting structures embed into Zilber fields.

All of this shows quite well the two obstructions that our method is not able to overcome: first of all, if $V \subset \mathbb{G}^n$, it is not always true that the topological dimension of $\begin{pmatrix} \mathrm{Id} & 0 \end{pmatrix} \cdot \check{V}$ is $2n$, so the argument of Lemma 12.3 does not work in the general case, and we cannot produce an order-preserving exponential function. This destroys continuity as well.

However, this argument shows that if we manage to strengthen Theorem 9.1 as in Proposition 12.5, namely, if we discover that the map $V \to M \cdot \check{V}$ is surjective also for larger varieties, then Proposition 12.6 would apply in all cases; hence, we would not need the density arguments and the second countability, as the work of Section 12.1 would be sufficient to get (CCP) without further complications. In particular, it would be possible to find involutions on Zilber fields of arbitrary cardinalities, using arbitrary real closed fields, and we would find models outside of the class described in Section 4. Work is in progress about finding such a generalization.

References

[1] Ayhan Gunaydin and Amador Martin-Pizarro. Generic points on exponential curves. 2010. arXiv:1003.4948.

[2] Philip Hall. On Representatives of Subsets. *Journal of the London Mathematical Society*, s1-10(1):26–30, 1935. doi:10.1112/jlms/s1-10.37.26.

[3] Jonathan Kirby. Finitely Presented Exponential Fields. 2009. arXiv:0912.4019.

[4] Jonathan Kirby, Angus Macintyre, and Alf Onshuus. The algebraic numbers definable in various exponential fields. 2011. arXiv:1101.4224.

[5] Vincenzo Mantova. Involutions on Zilber fields. *Rendiconti Lincei - Matematica e Applicazioni*, 22(2):237–244, 2011. doi:10.4171/RLM/598.

[6] David Marker. A remark on Zilber's pseudoexponentiation. *Journal of Symbolic Logic*, 71(3):791–798, 2006. doi:10.2178/jsl/1154698577.

[7] Ahuva C. Shkop. *On Pseudoexponential Fields and Schanuel's Conjecture*. Ph.d. thesis, University of Illinois at Chicago, 2010. URL: http://www.math.bgu.ac.il/~shkopa/thesis.pdf.

[8] Boris Zilber. Pseudo-exponentiation on algebraically closed fields of characteristic zero. *Annals of Pure and Applied Logic*, 132(1):67–95, 2005. doi:10.1016/j.apal.2004.07.001.